НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

Факультет інформатики та обчислювальної техніки
(назва факультету, інституту)

Кафедра автоматизованих систем обробки інформації і управління
(назва кафедри)

"На правах рукопису"
УДК *001-004.7*

«До захисту допущено»
Завідувач кафедри

_____ О.А.Павлов
(підпис) (ініціали, прізвище)

“____” _____ 20*18* р.

МАГІСТЕРСЬКА ДИСЕРТАЦІЯ

на здобуття ступеня магістра

за спеціальністю *122 Комп'ютерні науки та інформаційні технології*
(код та назва спеціальності)

спеціалізацією *Інформаційні управляючі системи та технології*
(код та назва спеціалізації)

на тему: *Аналіз безпеки автомобіля на основі моделі загроз*

Виконав: студент *VI* курсу групи ІС-61м
(шифр групи)

Чеканін Олексій Юрійович _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник *доц., к.т.н., доц. Жданова О.Г.* _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант *к.т.н., доц. Жданова О.Г.* _____
(науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018

ВСТУП

Сучасні авто пропонують величезну кількість цифрових можливостей та стають дедалі складнішими. Вони містять до 100 електронних компонентів управління, які з'єднані між собою різними шинами, щоб зменшити кількість необхідних кабелів. Інформаційні технології наразі займають центральне значення для багатьох додатків та послуг в нових автомобілях. За оцінками, витрати на програмне забезпечення та електроніку досягають 50% значення у виробництві автомобілів у 2015 році [2]. Але що більш важливо, це те, що вже сьогодні більше 90% усіх інновацій автомобілів зосереджено на програмному та апаратному забезпеченні [3]. До 2020 року очікується приблизно 220 млн. авто, які будуть обладнані мережевими системами.

В автівках преміум-класу можна знайти до 70 ЕКУ, з'єднаних декількома типами шин і програмне забезпечення яке займає до декількох сотень мегабайт.

Але разом з новими можливостями з’являються і супутні ризики. Мережеві системи (Bluetooth, Wi-Fi, 4G, GPS), які стали частиною сьогоденних авто значно збільшують можливість зловмисного втручання у загальну роботу. Дослідниками в галузі інформаційної безпеки вже зроблені дослідження стосовно можливості здійснити атаку на мережу автомобіля [4].

Іншим фактором є тенденція до збільшення обміну інформацією між автомобільними системами та зовнішнім світом. Технології комунікації "автомобіль-автомобіль" (Car to Car, C2C) [5] або автомобіль-інфраструктура (Car to Infrastructure, C2I) вже проектуються та з часом стануть повсякденними.

В 2014 році хакери змогли отримати контроль над системою Jeep Uconnect в Jeep Cherokee [6], що включає в себе навігацію, Wi-Fi та Bluetooth парування (pairing) з телефоном. На додачу гальма, двигун та система рульового керування могли бути під впливом зловмисника, залишаючи можливість для потенційної загрози в круїз-контролі, системі помічника паркування та системі запобігання аварії.

Toyota Prius 2014 року мала вразливості в системі Safety Connect, Bluetooth,

систему видаленого доступу без ключа, власній радіо- та стільниковій мережі. Гальма та система керування кермом знаходилися в тій ж самій мережі, що і Bluetooth, що створювало ризики для безпеки водія.

Розглядаючи ці тенденції та високі ризики пов’язані з безпекою таких швидкозмінних обчислювальних систем, інформаційна безпека для автомобілів є новою важливою областю досліджень: на відміну від звичайних стаціонарних ПК, успішне порушення безпеки в мережі автомобіля може не тільки викликати незручність і розкрити конфіденційні дані, але й також безпосередньо загрожувати життю своїх користувачів (водіїв, пасажирів) та навколишнього середовища [7-5].

Існують результати практичних випробувань [8-6] щодо здійснення атак на автомобільне обладнання та програмне забезпечення, наприклад, електронні компоненти управління в мережі CAN (Controller Area Network).

Все це обумовлює необхідність створення систем для інформаційної безпеки спрямованих саме на автомобільні засоби.

Одним з найдієвіших засобів моніторингу інформаційної безпеки є системи виявлення атак. Створення таких систем для апаратного забезпечення, що використовує протокол CAN наразі є актуальною задачею, оскільки раніше вони розроблялись для комп’ютерних мереж, тоді як автомобіль має власні особливості, які необхідно прийняти до уваги. Система виявлення атак - це програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними [9]. Протокол CAN обраний через його популярність у автомобільній індустрії, а саме те, що більшість інформаційних мереж в автомобілі використовують саме цей протокол.

Системи виявлення атак (СВА) проектуються з урахуванням особливостей захищуваної системи та вимог до безпеки. Для цього необхідно мати огляд архітектури електронних компонентів автомобіля та мереж в ньому, мати перелік вже знайдених вразливостей та приклади успішних атак на автомобілі. Наразі проектування СВА для автомобілів є актуальним питанням і вже існують дослідження на цю тему [10, 11].

Для категоризації та визначення пріоритетів загроз використовуються побудова моделі загроз - аналіз потенційних загроз, результатом якого є ідентифікація, перелік та їх пріоритети. Також важливим документом є поверхня атаки - це перелік вразливих місць в інформаційній системі, через які зловмисник може впровадити власні дані, змусити систему зробити дії, для яких у нього немає прав або витягнути дані з системи.

Якщо модель загроз є переліком потенційних загроз, то поверхня атаки вже список реальних атак та слабких місць в захищуваній системі. Варто зазначити, що ефективно побудувати поверхню атак можна лише за наявності моделі загроз.

Найефективнішою стратегією виявлення зловмисних дій в мережі вважається моніторинг дій та даних в ній та виявлення аномалій, тобто поведінки, яка не вважається нормальною. Для цього будується багатовимірний профіль користувача, що описує дійсну поведінку користувача чи компонентів в мережі. Але побудова профілю вимагає значного обсягу даних, що не завжди можливо.

Для створення профілю користувача добре підходять штучні нейронні мережі (ШНМ), оскільки вони здатні апроксимувати складні функції, навіть ті, що не відомі в аналітичному вигляді. Існують приклади успішного використання ШНМ в якості детектора аномальної поведінки [10;12-14]. Важливим питанням залишається вибір ознак для тренування нейронної мережі, оскільки дані передаються у вигляді пакетів, кожен з яких може бути цілком легальним і водночас частиною атаки. В роботах [10;12-14] використовуються різні вектори ознак, що свідчить про те, що вибір даних для навчання є відкритим питанням.

1 ОГЛЯД ВИКОРИСТАНИХ ТЕХНОЛОГІЙ

1.1 Огляд комунікаційних технологій в сучасних автомобілях

Ще наприкінці 1970-х років було розпочато впровадження інформаційних технологій в автомобіль у формі електронних компонентів управління (ЕКУ), щоб зробити його споживання палива більш ефективним. З часом з’явився широкий спектр автоматизованих функцій, починаючи від регулювання дзеркал і закінчуючи антиблокувальною системою. Останній розвиток в автомобільній промисловості — це провадження технології автопілоту. Найбільш провідні компанії оголосили, що будуть працювати над створенням автономних транспортних засобів, очікується, що технологія буде готова для масового користування вже в 2025 році. Ця тенденція призводить до того, що ще більше функцій водія стануть автоматизованими та виконуватися програмним забезпеченням. Для цього системи, що знаходяться всередині автомобіля, стають більше пов'язані один з одним, а також з іншими транспортними засобами та мережею Інтернет.

Той факт, що автомобіль отримав доступ до Інтернету означає, що він став ціллю хакерів, які потенційно можуть втручатися в роботу транспортного засобу або виконати довільний код, що може призвести до непередбачуваних наслідків.

Зараз автомобілі набувають все більше і більше можливостей і для цього вони стають обладнані датчиками та спеціалізованими комп’ютерами (ЕКУ). Всі ці пристрої повинні бути об’єднаними в мережу, щоб обмінюватися інформацією для загальної роботи автівки. Оскільки архітектура компонентів стала занадто складною, щоб просто з’єднати усе в одну мережу, ЕКУ та сенсори почали об’єднувати в окремі мережі, які в свою чергу можуть бути частиною іншої. Комунікаційні мережі надають можливість передавати дані ефективним чином, виявляти помилки при передачі даних, підтримувати канал зв’язку в робочому стані.

Автомобілі є системами, де безпека критично важлива і несправності в автомобілі можуть призвести до серйозних травм або смерті пасажирів або пішоходів поблизу. Тому вкрай важливо розробити механізми виявлення нападів на інформаційні системи автомобіля та захисту проти них. Традиційно в галузі

інформаційної безпеки виділяють системи виявлення атак (СВА), які проводять заходи для захисту обміну інформацією. СВА — це програмний або апаратний комплекс для моніторингу стану та подій в мережі або комп’ютері для виявлення зловмисних дій, які визначаються правилами або шаблонами. При роботі з ЕКУ доводиться мати справу з ресурсними обмеженнями, такими як обмежена обчислювальна потужність і обмежена кількість оперативної пам'яті, а також вимоги щодо сумісності між апаратним забезпеченням та зворотної сумісності транспортних протоколів та програмного забезпечення.

ЕКУ з’єднані в багато мереж, які використовують різні протоколи та навіть різні версії цих протоколів в залежності від потреб виробника. Вони об’єднані в локальні мережі і обмінюється інформацією для виконання своїх обов’язків та діагностики мережі. Існують спеціальні ЕКУ які виконують роль шлюзів - пристроїв, що приєднані до декількох мереж, основною метою яких є передача повідомлень із одної мережі в іншу.

Виділяють три основні групи ЕКУ [15]:

– вузли з вимогою реального часу реакції; приклади: модуль управлінння двигуном, модуль управління гальмами, анти-блокувальна система (Anti-lock braking system, ABS), електропідсилювач керма, подушки безпеки і так далі;

– вузли із середнім рівнем часу реакції; приклади: центральний замок, парктроніка, зовнішнє освітлення (фари, поворотники), датчики тиску в шинах;

– вузли другорядної важливості; приклади: навігаційна система, мультимедійна система і т.д.

Наразі в автомобілях використовуються наступні протоколи [16]:

– CAN [17] (Controller Area Network);

– LIN [18] (Local Interconnect Network);

– FlexRay [19];

– MOST (Media Oriented Systems Transport).

На рисунку 1.1 представлений приклад загальної архітектури ЕКУ в сучасному автомобілі, що використовують вищеозначені протоколи.

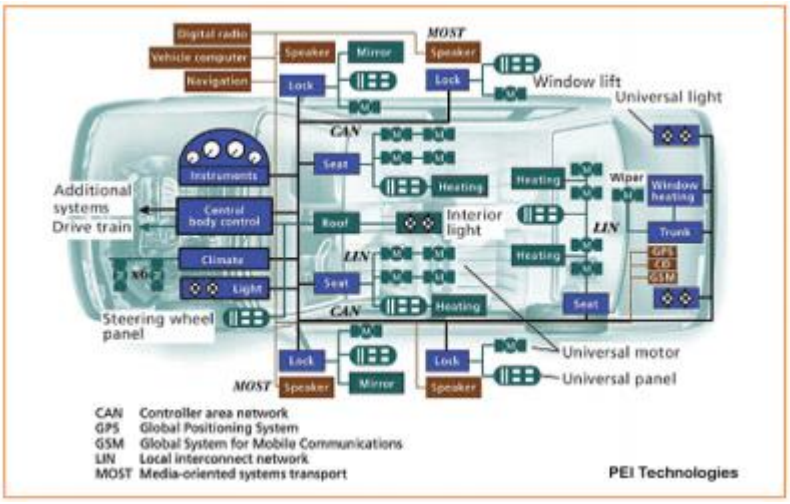

Рисунок 1.1 - Приклад загальної мережі автомобіля [21]

1.2 Огляд протоколів передачі даних

Найбільш поширеним протоколом є *Controller Area Network* [17], який можна вважити стандартом де-факто для обміну інформацією в автомобілі. Цей протокол було створено в середині 1980-х компанією Bosch. Зазвичай в автомобілі присутні дві або три окремі CAN мережі, що працюють з різною швидкістю передачі даних. ЕКУ з'єднані послідовною шиною і кожен компонент "бачить" кожне повідомлення в мережі.

CAN шина низької швидкості працює при менш, ніж 125 Кб/с та використовується для компонентів, які відповідають за комфорт, положення вікон, сидінь, інші можливості, які підбирає під себе користувач. Така шина має енергоефективний режим сну, в якому ЕКУ призупиняють відправку даних до того моменту, коли прийду повідомлення, що "розбудить" їх. Таким чином зменшується використання електроенергії акумулятора.

CAN шина високої швидкості призначена для критичної компонентів, які працюють в режимі реального часу (двигун, гальма, круїз-контроль). Максимальна швидкість передачі даних складає 1Мб/с. Нижче наведена типова структура ЕКУ[20], а на рисунку 1.2 архітектура ЕКУ у складі 4 мереж.

Типова структура ЕКУ має наступні елементи [22]:

– мікроконтролер, який відповідальний за генерацію та обмін даними з

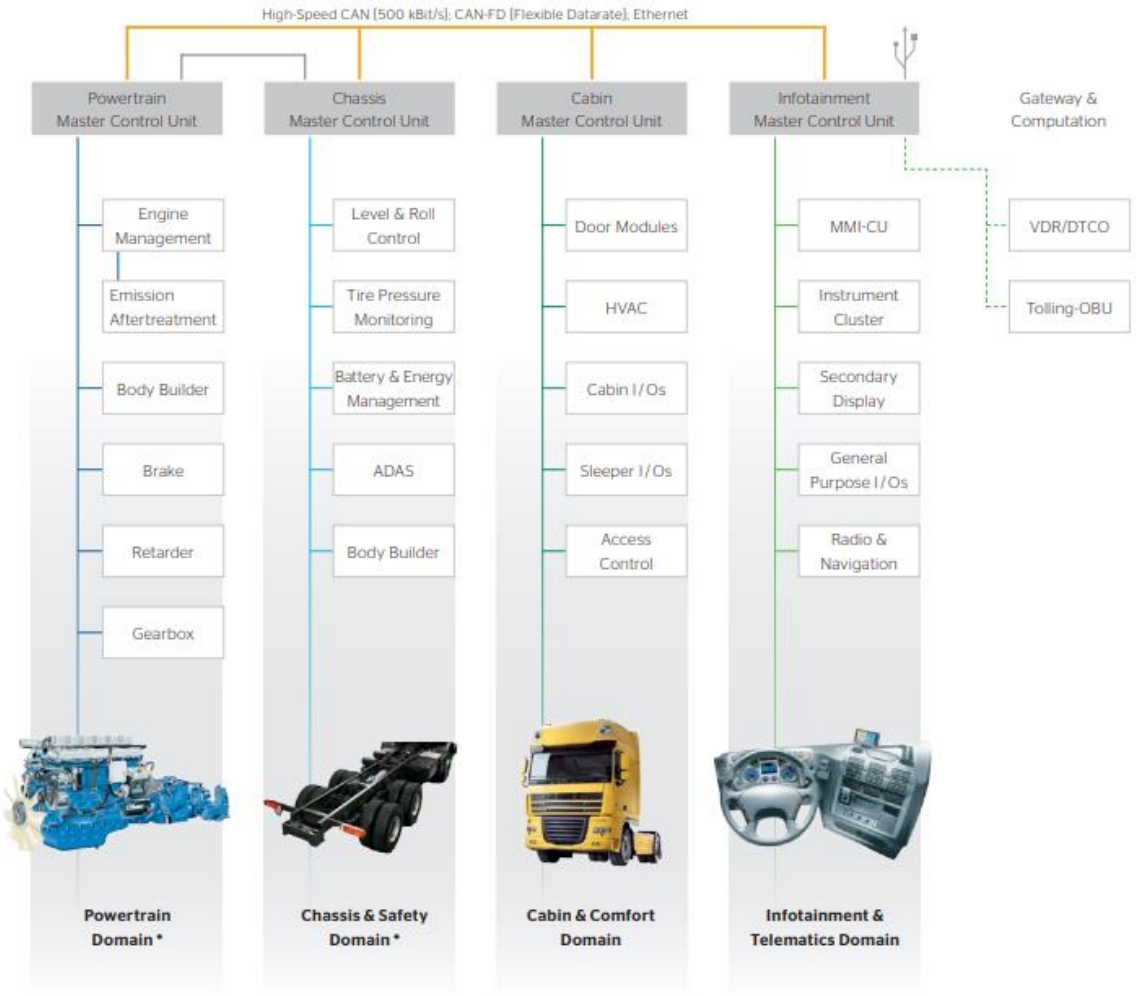

Рис. 1.2 - Приклад архітектури ЕКУ автомобіля [20]

іншими ЕКУ;

– контролер CAN; отримує та передає пакет в мережу, виконує вимоги протоколу стосовно доступу до шини.

– передавач CAN; транслює електричний сигнал в цифрове представлення для контроллера та навпаки;

Протокол *Local Interconnect Network* також працює через послідовну шину, що є схожою на CAN за принципом роботи. Відмінність у тому, що це є легшою для використання та впровадження технологією, а тому і дешевшою. Тому вона використовується для тих ЕКУ, що не є критично важливими.

FlexRay - це протокол, що перевершує CAN в передачі даних та надає високу швидкість комунікації для ЕКУ які працюють в умовах де час є критичним. Це

управління двигуном, гальмами, т. д. Порівняно з CAN протокол FlexRay був спроектований для більш швидкого та надійного обміну даними, він пропонує двох-канальну комунікацію та можливість утворювати різні топології: зірка, коло та інші. Але це призвело до удорожчання цієї технології порівняно з CAN.

Media Oriented Systems Transport (MOST) забезпечує високу швидкість обміну інформації та використовується для мультимедійних компонентів авто для передачі аудіо та відео. Мережі MOST побудовані за топологією кільце.

1.3 Специфікація передачі даних за протоколом CAN

Типи пакетів

Більша частина стандарту CAN зосереджується на рівні каналу передачі даних, що діє як інтерфейс між фізичним рівнем та вищими по відношенню до нього рівнями згідно з мережевою моделлю OSI [23]. Протокол передачі даних ретельно описано в документі специфікації Bosch, хоча з деякими двозначностями, які згодом були висвітлені в стандарті ISO 11898-1.

Стандарт описує чотири типи пакетів:

- пакети даних;
- віддалені пакети;
- пакети помилок;
- пакети перевантаження.

Пакети даних та віддалені пакети характеризуються двома варіантами: стандартним форматом (визначений у частині A для Bosch CAN 2.0[17]) та розширеному форматі (який використовує 29-розрядний ідентифікатор кадру, визначений у частині Bosch CAN 2.0 B[17]).

Пакет даних передає дані від передавача до всіх приймачів. Віддалений пакет надсилається вузлом для запиту нового пакету даних із надісланим ідентифікатором. Пакет помилки надсилається будь-яким вузлом, коли виявляється помилка в бітах повідомлення, помилка CRC, помилка формату або помилка підтвердження (або їх комбінація).

Пакет помилки складається з:

– позначка помилки: 6 біт, домінантних або рецессивних в залежності від поточного стану помилки контролера CAN;

– суперпозиція прапорів про помилки: можливе накладання прапорів помилок, відправлених різними контролерами в різні моменти;

– розділювальний символ: 8 рецессивних бітів, що вказують на кінець пакету помилок.

– призначення пакету перевантаження полягає у затримці передачі наступних пакетів даних або віддалених пакетів. Пакет перевантаження містить:

– позначку перевантаження: 6 домінуючих бітів;

– суперпозиція позначок перевантаження: можливого накладання позначок перевантаження, відправлених різними контролерами в різні моменти

– розділювальний символ: 8 рецессивних бітів, що сигналізують про кінець кадру перевантаження.

Контроль помилок

Усього є 5 різних типів помилок.

Бітова помилка: компонент, яка надсилає бітову послідовність по шині, також стежить за шиною. Бітова помилка повинна бути виявлена коли є відмінність в надісланих та виявлених бітах. Винятком є відправка рецесивного біта під час наповнення бітового потоку або під час сінхронізації. Бітова помилка не виникає, коли виявлений домінуючий біт.

– *помилка у змісті*: помилка з`являється коли надходять шість біт однакового рівня у полі повідомлення, яке слід кодувати методом наповнення бітів;

– *помилка CRC*: кожен пакет має CRC який розраховується передавачем, приймачі розраховують CRC так само, як і передавач; помилка CRC повинна бути виявлена, якщо розрахунковий результат не співпадає з отриманим у послідовності CRC;

– *помилка формату*: помилка з’являється, коли бітове поле з фіксованим форматом містить один або декілька помилкових бітів;

– *помилка підтвердження*: помилка підтвердження повинна бути

виявлена передавачем, коли він не виявляє домінуючий біт протягом синхронізації.

1.4 Комунікація автомобіля із зовнішнім світом

Наразі перспективними комунікаційними технологіями для обміну інформацією з іншими авто на дорозі (Авто-Авто, Vehicle-to-Vehicle, V2V), з дорожньою та міською інфраструктурою (Авто-Інфраструктура, Vehicle-to-Infrastructures, V2I) та спеціалізовані мережі автомобілів (Vehicle Ad-hoc Networks (VANETs)). Вони дозволяють по новому подивитись на автівки та перетворити їх на інформаційний хаб. Також постає питання про надійний та безпечний спосіб оновлення програмного забезпечення автомобіля через бездротові мережі (FOTA - Firmware Over The Air). На рисунку 1.3 зображені зовнішні інтерфейси сучасного автомобіля.

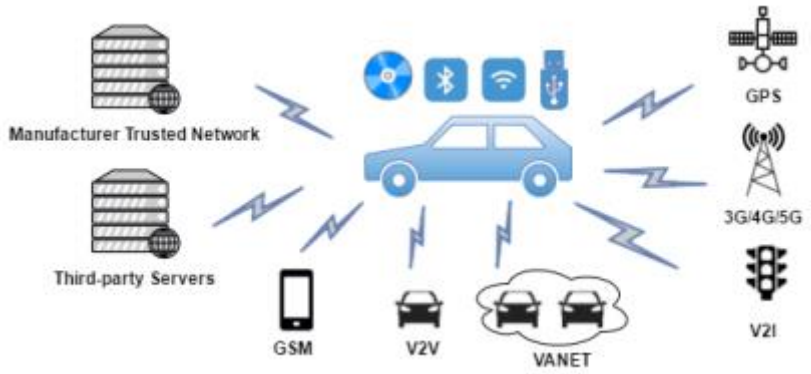

Рисунок 1.3 - Зовнішні канали зв’язку автомобіля [11]

1.5 Системи виявлення атак

Системи виявлення атак (СВА) - це програмний або апаратний засіб [24], призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними.

СВА можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти раніше невідомі атаки. Системи які не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки,

називаються системами запобігання атак. Якщо міжмережевий екран спрямований на захист об’єкта від зловмисника, який знаходиться поза мережею, то СВА аналізують інформацію та дії, що відбуваються всередині мережі. Правильність результатів та ефективність СВА можна оцінити за 4 параметрами (таблиця 1.1).

Таблиця 1.1 – Параметри роботи СВА

Параметр	Опис
Істинно позитивний (True Positive)	Дія була кваліфікована як атака і вона дійсно є зловмисною
Істинно негативний (True Negative)	Дія була кваліфікована як нормальна і вона дійсно нормальна
Хибно позитивна (False Positive)	Дія була кваліфікована як зловмисна, хоча в дійсності вона нормальна
Хибно негативна (False Negative)	Дія була кваліфікована як нормальна, хоча в дійсності є атакою

Найбільш важливим результатом серед усіх, що надає СВА є хибно негативний, оскільки наслідком є обман систем безпеки і те, що зловмисник вважається легітимним користувачем. Також під час проектування СВА вважливо зменшити кількість хибно позитивних результатів, щоб не ускладнювати аналіз попереджень від систем безпеки.

СВА вирішують наступні завдання [25]:

– розпізнавання відомих і, по можливості, невідомих атак та попередження про здійснення зловмисних дій;

– статистичний аналіз шаблонів аномальних дій;

– моніторинг і аналіз користувацької, мережевої та системної активності;

– контроль цілісності файлів та інших ресурсів захищуваної системи (ЗС);

– аудит конфігурацій та налаштувань;

– встановлення і підтримка роботи серверів-пасток для запису інформації про порушників;

– автоматизація рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами ЗС.

Для виконання вимог щодо забезпечення інформаційної безпеки (ІБ) СВА використовують наступні механізми [25]:

– політика ІБ;

– ідентифікація учасників процесу інформаційної взаємодії;

– контроль доступу учасників процесу інформаційного обміну до ресурсів і рівня цього доступу;

– аудит і моніторинг подій, що відбуваються в процесі обміну інформацією;

– реагування на інциденти при порушенні або підозрі на порушення ІБ;

– управління конфігурацією середовища інформаційного обміну відповідно до вимог ІБ;

– управління користувачами в середовищі інформаційного обміну відповідно до вимог ІБ;

– забезпечення стійкості середовища інформаційного обміну.

Класифікація систем виявлення атак

Виділяють наступні типи СВА:

– статичні;

– динамічні;

– мережеві;

– системні.

Статичні СВА роблять «знімки» захищуваної системи та середовища в якому вона знаходиться, здійснюють їх аналіз, розшукуючи вразливе ПЗ, помилки в конфігураціях і т. д. Йде перевірка версій прикладних програм на наявність відомих вразливостей і слабких паролів, вміст спеціальних файлів в директоріях

користувачів або конфігурацій відкритих мережевих сервісів. Статичні СВА виявляють сліди вторгнень.

Динамічні СВА здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі або мережі, переглядаючи файли аудиту або мережеві пакети, що передаються за певний проміжок часу. Ці системи реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Мережеві СВА контролюють пакети в мережі і виявляють спроби зловмисника проникнути всередину системи або реалізувати атаки. Ці системи працюють з мережевими потоками даних. СВА може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, що переглядає весь трафік у мережі (концентратор, маршрутизатор, тощо). Мережеві СВА контролюють багато комп'ютерів, тоді як інші типи контролюють тільки один.

СВА, які встановлюються на хостовому комп’ютері і виявляють зловмисні дії на ньому називаються *хостовими або системними* [24]. Прикладами хостових СВА можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Монітори реєстраційних файлів контролюють реєстраційні файли, створювані мережевими сервісами і службами.

Класифікація за джерелами даних

СВА зазвичай реєструють значну кількість даних, пов'язаних з виявленими подіями. Ці дані можуть бути використані для підтвердження обґрунтованості сповіщень, дослідження виявлених інцидентів та зіставлення подій з СВА та іншими джерелами даних. За джерелами даних СВА поділяються на наступні види:

Хостові (Host-based) контролюють трафік одного хоста та події, що відбуваються в мережі для виявлення підозрілої діяльності.

Мережеві (Network-Based) проводять моніторинг мережевого трафіку для певних сегментів мережі або пристроїв та аналізують трафік мережі. Типова архітектура мережевої СВА зображена на рисунку 1.4.

Гібридні системи поєднують в собі обидва види вищезазначених СВА які можуть використовуватися одночасно.

Системи, що засновані на аналізу поведінки в мережі (Network Behavior

Analysis) аналізують мережевий трафік для виявлення загроз, які створюють незвичні потоки трафіку, такі як розподілені атаки відмови в обслуговуванні, певні форми зловмисного програмного забезпечення та порушення політик безпеки.

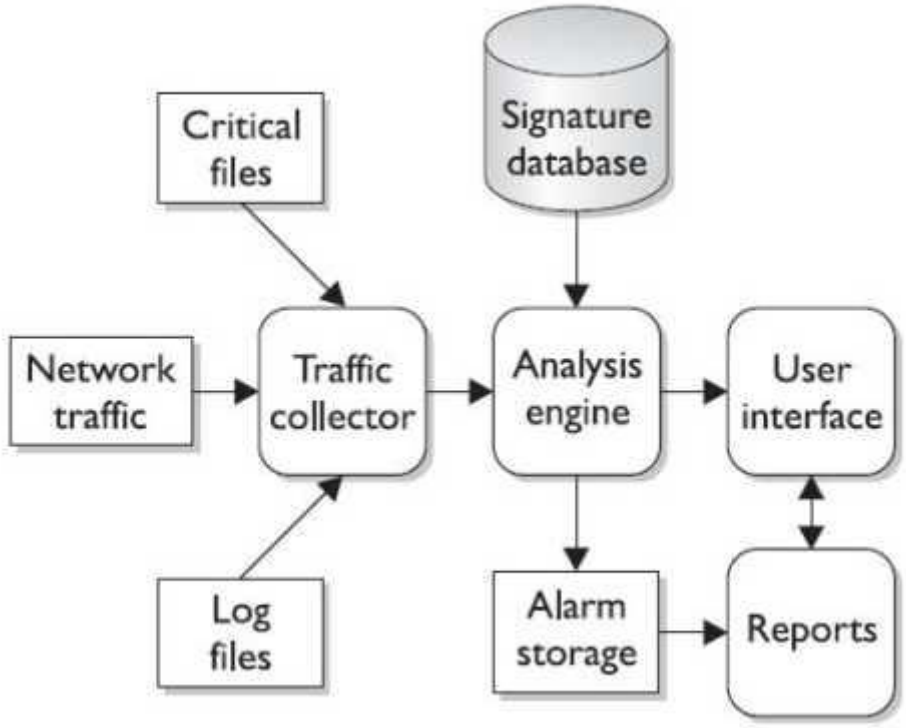

Рисунок 1.4 – Архітектура мережевої СВА [26]

Класифікація за способом виявлення атак

За способом виявленням загроз системи поділяються на ті, що базуються на сигнатурах та виявленні аномальної поведінки.

Виявлення основане на сигнатурах. Сигнатура атаки [27] — це характерні ознаки атаки або вірусу, що використовуються для їх виявлення. Основним способом виявлення зловживань є використання заздалегідь визначеної бази знань. Використовуються наступні методи виявлення:

– *виявлення основане на сигнатурах* (Signature based); відбувається пошук відповідності між наявними сигнатурами у базі знань з зібраними даними;

– *виявлення основане на правилах* (Rule based); система використовує набір правил логічного виводу "якщо-то" для класифікації комп'ютерних атак;

– *виявлення основане на переході станів* (State transition); система намагається ідентифікувати атаку, використовуючи скінченний автомат, який

виводиться на основі даних мережі; стан автомату відповідає різним станам мережі, а мережева подія спричиняє перехід у інший стан.

Аналіз сигнатур базується на простому понятті збігу виявлених даних зі зразком попередньо виявлених та доданих у систему атак. Метою є виявлення дій, команд, даних, що порушують політики безпеки.

Переваги:

– є дуже ефективними та не спричиняють хибно негативних результатів;

– надають системним адміністраторам легку можливість контролювати стан захищеності, навіть якщо вони не є експертами з інформаційної безпеки.

Недоліки:

– можуть виявляти тільки ті атаки, що заздалегідь відомі, тому повинні постійно оновлюватися для змоги знайти нові атаки;

– можуть виявляти лише тільки ті атаки, що були додані в СВА. Навіть відома атака із незначними змінами не буде виявлена.

Виявлення аномальної поведінки - це результат стратегії "аномалією є все, що не є нормальним". Найважливішим питанням є те, що вважати аномальною та нормальною поведінкою. Ці системи використовують наступні методи:

– *статистичні методи;* поведінка користувача та стан мережі спостерігаються шляхом вимірювання статистичних даних з часом;

– *методи основані на відстані;* метою цього методу є подолання обмежень статистичних методів, коли дані важко оцінити в багатовимірних просторах;

– *методи основані на правилах;* СВА має заздалегідь отримані знання про нормальну поведінку користувача та стан мережі, визначає зловмисну активність шляхом порівняння нормальної поведінки з поточними операціями користувача та станом мережі;

– *основані на профілі користувача*; цей метод схожий на метод, оснований на правилах, але в даному випадку створюється профіль нормальної поведінки для різних типів трафіку в мережі, користувачів та всіх пристроїв, а відхилення від цих профілів означає атаку; поведінка користувача та стан мережі представляються

багатовимірним вектором; створюється профіль користувача, що представлений багатовимірною сферою, якщо вектор, що представляє поведінку користувача виходить поза межі сфери, то поведінка вважається зловмисною;

– *Основані на моделюванні*; підходи, що ґрунтуються на відмінностях у нормальній та ненормальній поведінці, їх моделюванні, але без чисельних профілів.

Аналіз аномалій полягає в виявленні поведінки чи даних в мережі, що відрізняються від “нормальних”. В такому випадку будь-що, що відрізняється від нормальної поведінки в мережі розцінюється як атака і завдання таких СВА в виявленні відхилення від очікуваної поведінки. Системи виявлення аномалій будують профіль користувача використовуючи нормальну поведінку на основі даних під час нормальної роботи захищуваної системи. Під час роботи СВА стежать за подіями та даними в мережі, порівнюють їх з побудованим профілем та намагаються виявити відхилення. Ці відхилення позначаються як атаки.

Переваги:

– СВА, що відстежують аномалії здатні виявляти загрози, навіть якщо немає їх детального опису або вони ще невідомі;

– можуть бути використаними для отримання сигнатур для СВА, що базуються на сигнатурах.

Недоліки:

– створюють багато хибно позитивних результатів, оскільки справжні дії користувача не завжди відомі заздалегідь;

– вимагають велику кількість діагностичних даних для побудови профілю користувача.

1.6 Огляд штучних нейронних мереж

Штучні нейронні мережі (ШНМ) – це математичні моделі [28], а також їх програмні або апаратні реалізації, побудовані за принципом організації й функціонування біологічних нейронних мереж – мереж нервових кліток живого організму. Це поняття виникло при вивченні процесів, що протікають у мозку, і при

спробі змоделювати ці процеси.

ШНМ являють собою систему з'єднаних і взаємодіючих між собою простих процесорів (штучних нейронів). Такі процесори звичайно досить прості, особливо в порівнянні із процесорами, використовуваними в персональних комп'ютерах. Кожний процесор подібної мережі має справу тільки із сигналами, які він періодично одержує, і сигналами, які він періодично посилає іншим процесорам. Проте, з'єднавши їх в досить велику мережу з керованою взаємодією, такі локально прості процесори разом здатні виконувати досить складні завдання.

З погляду машинного навчання, нейронна мережа являє собою окремий випадок методів розпізнавання образів, методів кластеризації й т.п. З математичної точки зору, навчання нейронних мереж – це багатопараметричне завдання нелінійної оптимізації. З погляду кібернетики, нейронна мережа використовується в завданнях адаптивного керування і як алгоритми для робототехніки. З погляду розвитку обчислювальної техніки й програмування, нейронна мережа – спосіб розв'язку проблеми ефективного паралелізму.

Інформація в мережі кодується і запам’ятовується не в окремих елементах пам’яті, а в розподілі зв’язків між нейронами і в їх силі, тому стан кожного окремого нейрона визначається станом багатьох інших нейронів, пов’язаних з ним. Отже, втрата одного або декількох зв’язків не робить істотного впливу на результат роботи системи в цілому, що забезпечує її високу надійність [29].

ШНМ використовуються для вирішення наступних проблем [28]:

- обробка і аналіз зображень;
- розпізнавання мови незалежно від диктора;
- обробка високошвидкісних цифрових потоків;
- автоматизована система швидкого пошуку інформації;
- класифікація інформації в реальному масштабі часу;
- планування, застосування сил і засобів у великих масштабах;
- вирішення трудомістких задач оптимізації;
- адаптивне управління і передбачення.

Функція витрат є важливим поняттям у навчанні, оскільки вона є мірою того,

наскільки далеким є певний розв'язок від оптимального розв'язку задачі, яку потрібно розв'язати. Алгоритми навчання здійснюють пошук простором розв'язків, щоби знайти функцію, яка має найменші можливі витрати.

Для тих застосувань, де розв'язок залежить від даних, витрати обов'язково мусять бути функцією від спостережень, бо інакше модель не матиме зв'язку з даними.

1.7 Особливості використання ШНМ в якості детектора аномальної поведінки

Найпростішим способом виявлення аномальної поведінки це використання правил логічного виводу “якщо-то”, які діють за принципом — якщо умова в правилі вірна, то аномалія виявлена. Хоча це і є дієвим та ефективним з точки зору швидкодії та опису атак способом, він не здатний виявити нові або неописані правилами аномальні дії. Ця проблема є доволі критичною, оскільки атака, яка не підпадає під умови правил, виявляється розробниками СВА пізніше, ніж вона вперше проводиться. До того будь-яка нова атака призводить до необхідності створення нових правил, що також вимагає часу та зусиль.

Штучні нейронні мережі дозволяють вирішити це питання за рахунок того, що вони здатні навчитися нормальній поведінці, що не передбачена розробниками та виявляти відхилення від звичних дій.

Ще однією перевагою є здатність ШНМ представляти складні аналітичні функції, в контексті СВА, профіль користувача, що є складною задачею під час розробки профілю розробниками СВА.

ШНМ здатні обробляти інформацію, природа або зміст якої невизначена заздалегідь, навіть якщо дані пошкоджені або надходять у невірному порядку.

У випадку з комп’ютерними мережами, інформація може надходити від чисельних вузлів мережі і здатність обробляти нелінійні залежності стає вкрай важливою. До переваг нейронних мереж також відноситься і швидкість виявлення атаки (після навчання).

Проте існують і недоліки [30] у використанні ШНМ в СВА.

Високі вимоги до тренування. Здатність нейронної мережі виявляти аномальну поведінку в першу чергу залежить від навчання мережі, даних для навчання та способу у який відбувається навчання.

Навчання вимагає значного обсягу даних (десятки тисяч векторів для тренування) для того, щоб мережа була здатна навчитися виявляти різні класи атак та нормальну поведінку.

Для кожного класу аномальної поведінки необхідно розробити послідовність дій, що моделюють атаку так само, як вона буде проводитися під час роботи СВА. Чим більше можливих атак, тим більше необхідно даних і часу для навчання.

ШНМ діє як "чорний ящик". На відміну від експертних систем [31] з прописаними чіткими правилами, параметри нейронної мережі змінюються під час навчання для адаптації під вимоги під час навчання. Після того, як мережа здатна надавати задовільний рівень помилок, її параметри більше не змінюються, проте неможливо чітко сказати наскільки точними є її відповіді.

Використання ШНМ у складі СВА поділяється на два типи [30]:

– нейронна мережа фільтрує дані і у разі виявлення атаки, дані потім передаються до експертної системи для додаткової ідентифікації;

– нейронна мережа отримує вхідні дані і сама приймає рішення чи містять вони ознаки аномальної поведінки. У разі виявлення неавторизованих дій відправляється повідомлення до системного адміністратора або спрацьовує система попередження атак.

1.8 Використання ШНМ в складі СВА

Існують приклади [12] успішного використання ШНМ для виявлення аномальної поведінки в захищуваній системі. Варто зазначити, що вищеозначені роботи переважно зосереджені для роботи з комп'ютерними мережами. Використовувались чисельні архітектури ШНМ, серед яких:

– перцептрон;

– багатошаровий перцептрон;

– самоорганізаційна карта Кохонена;

– опорно-векторні машини.

Основними питаннями, що постають перед дослідниками є стратегія за якою ознаки вилучаються з вхідних даних та генерація даних для навчання і тренування. Для отримання ознак для навчання можливі 2 стратегії:

– вхідні дані не підлягають додатковій обробці (фільтрування, зменшення розмірності, тощо) і передаються на вхід нейронної мережі. Мережа навчається вилучати ключову інформацію із тих даних, що використовуються в захищуваній системі;

– дані від захищуваної системи спочатку обробляються (вилучаються окремі ознаки, фільтруються, зменшується розмірність даних) і після цього формується вектор ознак для подальшого навчання.

ШНМ може навчатися певним закономірностям в даних чи поведінці користувача або кластеризувати дані, що відповідають заданим умовам серед загального потоку даних.

Чим більш дані для навчання схожі на ті, що використовуються на практиці, тим більше здатність мережі виявляти реальні дані. Нажаль не завжди набори даних є в відкритому доступі і доводиться створювати дані штучно для моделювання роботи та середовища, в якому знаходиться захищувана система.

Необхідно зазначити, що дані від захищуваної системі можуть братися по одному вектору (як це зроблено в цій роботі згідно з особливостями протоколу CAN) або збиратися протягом проміжку часу [14]. В другому випадку неможливо передати мережі дані без попередньої обробки.

Архітектура ШНМ залежить від кількості класів які повинна розпізнавати мережа. Наприклад перцептрон здатний лише розрізнити нормальну та аномальну поведінку, що робить неможливим його використання в разі необхідності виявляти атаки, що відрізняються між собою. В даній роботі розглядаються нормальна поведінка та п’ять типів атак (див. розділ 3.8), саме тому використовувався багатошаровий перцептрон через його здатність до багатакласової класифікації.

Висновок до розділу 1

В даному розділі наданий огляд електронних компонентів управління та протоколів обміну даними, що використовуються в транспортних засобах, можливостей інформаційних систем автомобіля. Були розглянута класифікація систем виявлення атак за параметрами, що описують середовище в якій працює СВА та способу виявлення неавторизованих дій. Було обрана архітектура мережевої СВА, що виявляє аномальну поведінку для захисту ЕКУ автомобіля, які використовують протокол CAN для обміну даними. Розглянуті завдання, які вирішують штучні нейронні мережі, їх використання в якості детектора аномальної поведінки у складі СВА. Обрано багатошаровий перцептрон для використання в якості бази правил та детектора системи виявлення атак.

2 АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМОБІЛЯ

2.1 Важливість захищеності та безпеки

Чисельні рішення та заходи для інформаційної безпеки для комп'ютерів та мобільних пристроїв вже стали повсякденними. В той же час захищеність автомобілів, які за останні роки стали не менш комп'ютеризованими, залишається поза увагою. Незважаючи на те, що виробники автомобілів протягом останніх десятиліть покращили захищеність своїх автомобілів від автомобільних аварій, наразі відсутні цілісна концепція інформаційної безпеки. На даний час, механізми безпеки на основі шифрування або цифрових підписів вже можуть бути знайдені в сучасних автомобілях [32], але лише в дуже локальних масштабах, захищаючи окремі компоненти або функції.

Сенатор США Ед Маркі представив доповідь [33] присвячену проблемам інформаційного захисту саме у контексті сучасного стану автомобілів та відношення виробників до безпеки. Сенатор надіслав запитання стосовно атак на автомобіль через бездротові технології, заходів, що вживають виробники та їх можливостей стосовно виявлення неавторизованих дій. Запит був надісланий 16 автовиробникам: BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (разом з Audi) та Volvo. За результатами відповідей були зроблені наступні висновки.

Висновок 1. Майже 100% автомобілів, що представлені у продажу, обладнані бездротовими технологіями передачі даних. Це створює потенційні загрози для інформаційної безпеки.

Висновок 2. Більшість виробників не мають змоги отримати інформацію про атаки, що були здійснені на автомобіль в минулому.

Висновок 3. Заходи з інформаційної безпеки, що здійснюють виробники, не можуть вважатися достатніми, також вони не є системними, а залежать виключно від рішення виробника. Більшість виробників не змогли надати чітку відповідь стосовно того, як забезпечується інформаційна безпека, а саме: була надана загальна відповідь без жодних конкретних деталей, або питання взагалі проігноровано.

Експерти дійшли до висновку, що з 7 заходів 5 не можуть вважатися надійними [33]. Лише 7 виробників перевіряють виконання заходів з безпеки (хоча і за допомогою сторонніх компаній), в той час як 5 компаній не роблять цього, а 4 проігнорували це питання. Також виявилося, що оновлення ПЗ автомобіля відбувається лише в сервісних центрах і відсутня можливість надіслати діагностичну інформацію через Інтернет.

Висновок 4. Тільки 2 компанії обладнують автомобіль можливістю реагувати на неавторизовані або аномальні дії в режимі реального часу. Інші ж виробники покладаються на інструментарій, що не призначений для цих цілей. Виробниками додані функції моніторингу та мережевого екрану в ЕКУ, що лише дозволяє виявити незвичну поведінку в мережі, тоді як зміст даних жодним чином не аналізується.

Висновок 5. Автомобіль збирає значну кількість інформації про водія та роботу автомобіля. До цих даних відносяться географічне положення, місця паркування, інформація про прискорення, використання руля, гальм, пасока безпеки, швидкість та напрямок руху автомобіля. Було також показано, що в 2014 році збільшився відсоток автомобілів, що збирають інформацію про водія та те, як він використовує транспортний засіб.

Висновок 6. Більшість автовиробників збирають та передають дані під час користування автомобілем в центри даних, включаючи сторонні, і вони не були в змозі описати яким чином захищаються ці дані. Половина з компаній зберігає ці дані поза межами автомобіля. Відсутність загального підходу та вимог до збору, передачі та зберігання цих даних призводить до того, що кожний автовиробник вирішує ці питання сам. Як наслідок, не можливо оцінити дії виробників за певними критеріями, що породжує потенційні загрози.

Висновок 7. Виробники використовують персональні дані так, як вони вважають доцільним, не надали чіткої відповіді які дані використовуються та як, користуються послугами сторонніх компаній і самі вирішують скільки ці дані зберігаються та згідно з якими політиками безпеки. Можна сказати, що індустрія виробників транспортних засобів не має визначених правил та політик по відношенню до використання даних про водія та роботу автомобіля.

Висновок 8. Водії часто не мають повного уявлення про те які дані збираються під час користування автомобілем і можливі ситуації, коли вони не мають змогу відмовитися від збору інформації для користування функціями автомобіля, наприклад, навігацією.

Багато класичних технологій уже добре зарекомендували себе в автомобільній промисловості, наприклад, спільний дизайн апаратного та програмного забезпечення, повторне використання програмного забезпечення та його безпека. Проте одному аспекту сучасних інформаційних систем приділяється мало уваги в контексті автомобільних застосувань: інформаційна безпека.

Необхідно зазначити різницю між безпекою та захищеністю інформаційних систем автомобіля. Захищеність відноситься до технічних несправностей, тоді як безпека стосується протидії зловмисним та неавторизованим дія. Слід додати, що вони є пов’язаними галузями, тобто деякі технічні несправності (проблема захищеності) можуть бути використані для реалізації певної зловмисної загрози (проблеми безпеки) і навпаки [32].

Більшість програмних і апаратних систем сучасних автомобілів не захищені від зловмисних дій. Причиною цього є те, що донедавна автомобілі не потребували таких функцій через малий стимул до зловмисних дій. По-друге, безпека зазвичай на другому плані в будь-якій інформаційній системі, оскільки основний функціонал часто є головним завданням при розробці системи.

Наступні можливості вже скоро можуть з'явитися у транспортних засобах:

– можливість для перепрограмування зростаючої кількості ЕКУ з захистом кожного компонента;

– електронні протиугінні заходи будуть здійснюватися шляхом захисту окремих компонентів;

– збільшення кількості законодавчих вимог (безпечні функції екстреного виклику);

– створення нових бізнес-моделей (обмежені за часом функції автомобілів або інформаційно-розважальний контент);

– автомобілі будуть обмінюватися даними з навколишнім середовищем

бездротовим способом, що потребує захищеного зв'язку між автомобілем та дорожньою інфраструктурою;

– розширення мережі автомобілів робить можливою комунікацію між автомобілями, які повинні бути захищені від зловживань та порушень конфіденційності.

Нижче наведено короткий список функціональних можливостей систем безпеки, які необхідні сучасним автомобілям:

– безпечне оновлення програмного забезпечення ЕКУ;
– запобігання несанкціонованого налаштування ЕКУ;
– запобігання несанкціонованої зміни пробігу;
– запобігання використання неоригінальних запчастин.

2.2 Проблеми безпеки протоколу CAN

Протокол CAN має ряд властивих слабких місць, які є загальними для будь-якої реалізації. Розглянемо ключові серед них [34].

Широкомовна передача. Оскільки пакети CAN передаються фізично та логічно для всіх вузлів, зловмисник, який отримав доступ до мережі може легко переглянути всі повідомлення або відправляти пакети до будь-якого іншого вузла мережі.

Вразливість до атаки «відмова в обслуговувані». Протокол CAN надзвичайно уразливий для атак на відмову в обслуговуванні. Кожен ЕКУ має власний ідентифікатор, що представлений числом. Чим менше це число, тим більший пріоритет мають пакети від цього ЕКУ. Схема арбітражу CAN на основі пріоритетів дозволяє вузлу встановлювати "домінуючий" стан на шині і викликати відмову всіх інших вузлів шини CAN. Тобто зловмисник може надсилати пакети з найменшим можливим ідентифікатором і дані від інших ЕКУ не будуть пересилатися взагалі.

Відсутність відміток про аутентифікацію. Пакети протоколу CAN не містять поля аутентифікації або навіть будь-якого поля ідентифікатора джерела

пакета. Це означає, що будь-який компонент може надіслати пакет з ідентифікатором будь-якого іншого компонента. Будь-який скомпрометований компонент може використовуватися для управління всіма іншими компонентами в мережі.

Слабкий контроль доступу. ЕКУ використовують протоколи безпеки, де спочатку відбувається обмін даними для створення спільного криптографічного ключа. Проте було показано, що не всі ЕКУ використовують випадкові значення кожного разу або взагалі вимагають наявності ключа. Також в якості ключа можуть бути використані звичайні слова або вирази замість випадкових значень.

Вразливість обробки помилок. Вразливість полягає в обробці бітових помилок. Згідно зі специфікацією CAN, бітова помилка трапляється коли передавальний вузол CAN, який, за протоколом, повинен контролювати сигнал шини кожного разу, коли він транслює пакет, якщо значення на шині відрізняється від бітового значення, яке він намагається надіслати. Якщо вузол спостерігає такий стан, він повинен перервати передачу і негайно відправити пакет помилки. Це приводить до того, що всі інші вузли відхиляють отриманий до цього моменту пакет, фактично заперечуючи прийом цього кадру. Тоді передавальний вузол повинен повторити передачу.

Як наслідок, оскільки в CAN мережі всі вузли здатні фізично взаємодіяти один з одним, то за специфікацією будь-який компонент, підключений до шини, здатний відхилити пакет раніше відправлений по шині будь-яким іншим вузлом.

2.3 Потенційні контрзаходи

Існуючі аспекти інформаційної безпеки повинні розглядатися під час виявлення слабких місць та підвищення функціональності безпеки автомобіля:

- конфіденційність / приватність;
- цілісність;
- наявність;
- автентичність;
- безвідмовність.

Оскільки транспортні засоби мають власні особливості, вони потребують спеціальних вимог до безпеки. Для забезпечення безпеки дорожнього руху та експлуатаційної надійності транспортних засобів визначені наступні загальні цілі:

– конфіденційність даних: неавторизований доступ до захищених даних повинен бути заблокованим;

– цілісність даних: неавторизована модифікація даних повинна бути заблокованою або принаймні виявленою;

– цілісність апаратного та програмного забезпечення: несанкціонована модифікація апаратного або програмного забезпечення повинна бути нездійсненною або принаймні виявленою;

– наявність: авторизовані апаратні та програмні компоненти повинні мати належний доступ до даних та послуг, що вони потребують для нормального функціонування;

– унікальність: несанкціоноване клонування апаратних компонентів повинно бути нездійсненним або принаймні виявлено.

Конфіденційність та приватність. Повідомлення, надіслане через шину CAN, може бути отримано усіма іншими ЕКУ, підключеними до цієї шини. На підставі ідентифікатора компонента, кожен ЕКУ вирішує використовувати пакет або ігнорувати. Інформація, що може передається може вважатися конфіденційною, зібравши інформацію з шини CAN, зловмисник може, наприклад, вилучити конфіденційну інформацію про водія або під час діагностичних сеансів, навіть про попередніх водіїв. Такі заходи, як шифрування та анонімність даних зменшать означені загрози.

Цілісність. Протокол CAN забезпечує цілісність пакетів за допомогою циклічного надлишкового коду [35] (Cyclic Redundancy Checksum, CRC), але таким чином лише перевіряється цілісність переданих байтів, а не інформаційного вмісту. Зловмисник здатний створити власне повідомлення, упакувати його в пакет CAN і розрахувати CRC, і цей пакет буде дійсним. Усі інші ЕКУ будуть вважати начебто він надісланий дійсним компонентом. Існують належні заходи для збереження змісту, такі як криптографічні хеш-функції, коди аутентифікації повідомлень

(Message Authentication Codes, MAC) або цифрові підписи, які не можуть бути «перебудовані» зловмисником без знання секретного (приватного) ключа.

Автентичність. Протокол CAN не забезпечує жодних заходів автентичності, а повідомлення навіть не містять адреси відправника. Це дозволяє зловмисним вузлам легко надсилати повідомлення, які надсилають інші ЕКУ. Приймальні пристрої не мають можливості визначити, що дані постачаються з недостовірного джерела, а отже довіряють підробленому вмісту і виконують неавторизовані дії.

Наявність. Використання таких методів, як повторне надсилання індикаторів про помилку або високо пріоритетних повідомлень, дозволяє зловмисному вузлу перевантажувати всю мережу CAN. Під час атаки “відмова в обслуговуванні” жоден з інших пристроїв у цій мережі не буде доступний. Забезпечення доступності в таких умовах є складною проблемою. Специфікація протоколу FlexRay [9] містить можливість відключення несправних пристроїв або ліній від мережі вузлами - локальними або центральними "охоронцями шини".

Безвідмовність. Після інциденту, пов’язаному з підробкою ідентифікатора ЕКУ або даних, атаковані пристрої не мають можливості підтвердити того, що вони дійсно отримали дані від зловмисника або відповідно не надсилали такого повідомлення). Тому в разі порушення роботи внутрішньої системи транспортного засобу є вкрай складним визначити які компоненти скомпрометовані, а які - ні.

2.4 Моделювання загроз

Перед розглядом аналізу загроз необхідно привести визначення основних термінів, що використовуються далі:

– *кібератака* - напад на безпеку системи, що випливає з використання загрози, тобто інтелектуальної дії, що є навмисною спробою уникнути служб безпеки та порушити політику безпеки системи [36];

– *загроза* - можлива причина інциденту, що може призвести до шкоди системам і організації [37];

– *вразливість* - вада або недолік в дизайні системи, реалізації, або

операція та управління, які можуть бути використані для порушення політики безпеки системи [36].

Моделювання загроз - це процедура оптимізації безпеки мережі шляхом визначення цілей зловмисника та вразливостей, з подальшим визначенням контрзаходів для запобігання чи пом'якшення наслідків загроз для системи. У цьому контексті загроза являє собою потенційну або фактичну побічну подію, яка може бути шкідливою (наприклад, атакою на відмову в обслуговуванні) або випадковою (наприклад, збою пристрою зберігання даних), що може спричинити небезпеку для захищуваної системи.

Ключовий момент моделювання загроз полягає в тому, щоб визначити, де слід застосувати найбільше зусиль для забезпечення безпеки системи. Цей показник змінюється, коли додаються нові фактори, додається, видаляється або оновлюється програмне забезпечення, та розвиваються вимоги користувачів. Моделювання загрози - це ітеративний процес, який полягає у визначенні захищуваних активів, визначення того, що кожна програма робить щодо цих активів, створення профілів безпеки для кожної програми, визначення потенційних загроз, визначення пріоритетів потенційних загроз та документування побічних явищ та дій, здійснених у кожній із них.

Для створення моделі загроз використовуються методологія моделювання загроз для автомобіля [38], що базується на вимогах стандартів безпеки для транспортних засобів, та результати здійснення атак [34, 39, 40] на автомобілі, що присутні на ринку.

2.5 Стандарти безпеки транспортних засобів

Разом з все більшим використанням ЕКУ та більшої інтеграції інформаційних технологій в транспортний засіб, збої більше не стосуються зносу або порушенням електричних мереж, а помилкам програмування. Той факт, що електронні компоненти можуть впливати на фізичний світ, змусили виробників транспортних засобів та урядові організації визначити стандарт, згідно з яким виробники автомобілів повинні здійснювати роботу з ризиками. З цією метою в 2011 році

стандарт ISO 26262 був прийнятий на базі вже існуючого стандарту IEC 61508, який був розроблений для кібер-фізичних систем та був змінений, щоб бути більш придатним для транспортних засобів [41].

ISO 26262 визначає функціональну безпеку електричних та електронних систем у транспортних засобах і вважається стандартом для функціональної безпеки автомобіля.

Аналіз ризиків та оцінка ризиків

Першим кроком в ISO 26262 є іденти аналіз ризиків та оцінка ризиків (Hazard Analysis and Risk Assessment, HARA). Цей процес відбувається у два етапи:

- аналіз того, які небезпечні ситуації можуть виникнути
- оцінювання ризиків цих небезпек.

Хоча ISO 26262 не вказує конкретні способи виконання HARA, загальними техніками, які використовуються є проведення мозкового штурму можливих небезпек та використання технік, що оцінюють ризики небезпек, розглядаючи три аспекти:

- *ступінь тяжкості* небезпеки, наприклад, чи є небезпека життю людей;
- *вплив* небезпеки або наскільки імовірною є небезпека;
- *контрольованість* небезпеки; чи здатен водій запобігти небезпеці, наприклад, шляхом гальмування.

Разом ці аспекти визначають рівень цілісності безпеки автомобіля (Automotive Safety Integrity Level, ASIL) для кожної небезпеки.

Структура керування ризиками NIST/NHTSA (NIST/NHTSA Risk Management Framework). Ця структура керування ризиками [42] розроблена Національною адміністрацією безпеки дорожнього руху США (National Highway Traffic Safety Administration) та Національним інститутом стандартів і технологій США (National Institute of Standards and Technology, NIST). Вона забезпечує упорядкований та структурований спосіб для інтеграції заходів інформаційної безпеки та управління ризиками в життєвий цикл розробки. Послідовність цих етапів зображена на рисунку 2.1. Структура включає в себе шість етапів:

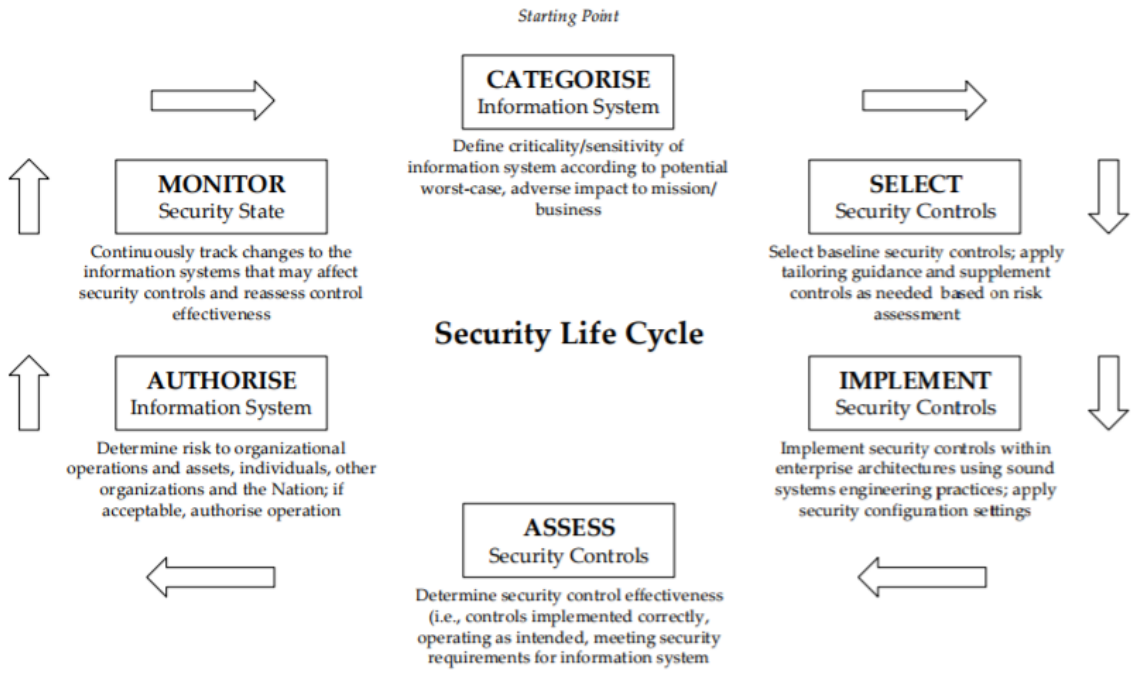

Рисунок 2.1 – Етапи NIST Risk Management Framework [42]

– *класифікувати* інформаційні системи та визначити критичність / чутливість інформаційної системи на основі аналізу впливу;

– *обрати* набір базових елементів керування безпекою та адаптувати або доповнити, якщо необхідно, на основі оцінки ризиків;

– *реалізувати* та описати заходи безпеки, використовуючи методи інженерії та застосувати засоби конфігурації безпеки;

– *оцінити* контроль безпеки для визначення ефективності управління, тобто чи правильно виконані заходи безпеки, чи працюють вони у відповідності до намічених цілей та відповідають вимогам безпеки інформаційної системи;

– *дозволити* інформаційній системі доступ до активів, фізичних осіб, інших систем на основі визначення ризиків для виконуваних операцій;

– постійно *контролювати* заходи безпеки та заново оцінювати ефективність управління, у тому числі звітувати про стан безпеки для відповідальних посадових осіб.

Була створена структура адаптована до вимог автомобільної індустрії, де був прибраний етап дозволу доступу до ресурсів, оскільки він не може бути застосований для систем автомобіля. Ця структура базується на існуючих

структурах NIST SP 800-37, NIST SP 80-39 та NIST SP 800-30.

Також існує потреба в кроці перед категоризації, на якому оцінюється система за допомогою моделі загрози та випадків використання. Цей перший крок має бути спрямований на кібер- або фізичні атаки, людські помилки, природні та техногенні катастрофи. З огляду на це, фахівці з безпеки можуть визначити набір характерних загроз, які можна класифікувати за чотирма можливими напрямками:

- конфіденційність;
- фінансові ризики;
- операційні ризики;
- безпека водія.

2.6 Модель класифікації загроз STRIDE

Класифікація загроз STRIDE [43] була розроблена корпорацією Microsoft і використовувалась як частина їх концепції життєвого циклу безпечної розробки для класифікації та виявлення потенційних загроз. Це акронім для наступних шести категорій загроз:

- підроблення ідентичності (**Spoofing identity**); зловмисник проводить неавторизовані дії від імені легітимного користувача;
- порушення даних (**Tampering with data**); зловмисник змінює довільним чином дані, що передаються між компонентами захищуваної системи;
- відмова від обов'язків (**Repudiation**); зловмисник намагається ініціювати події, що є недоступними або неприпустимими при поточних правах користувача;
- розкриття інформації (**Information disclosure**); зловмисник має можливість отримати дані в відкритому виді, доступ до яких йому заборонений;
- відмова в обслуговуванні (**Denial of service**); дії зловмисника призводять до того, що компоненти захищуваної системи не виконують

очікуваних дій на вимогу легітимного користувача або він має обмежений доступ до ресурсів, якими він володіє;

– перевищення привілеїв (**Elevation of privilege**); зловмисник отримує більші повноваження для взаємодії з захищуваною системою, ніж це передбачається політиками безпеки. Зловмисник має можливість ініціювати дії, які не повинні йому бути доступними.

Ідея класифікації STRIDE полягає в тому, щоб надати експертам із питань безпеки або тим, хто не є спеціалістом з питань безпеки інструменти для аналізу загроз безпеці. Вони використовує підхід в якому розглядається мета зловмисника. Наприклад, чи зможе він використати дані легітимного користувача для доступу Інтернет ресурсів (база даних, веб-сайт, тощо), чи можливо вилучити конфіденційну інформацію з даних, що передаються між компонентами захищуваної системи. В таблиці 2.1 наведено співвідношення між класами класифікації STRIDE та елементів діаграм потоку даних автомобіля.

Таблиця 2.1 – Застосування STRIDE до компонентів автомобіля

		Клас методології STRIDE				
Елемент	S	T	R	I	D	E
ЕКУ	✔	✔	✔	✔	✔	✔
Потік даних		✔		✔	✔	
Зовнішній елемент	✔		✔			

2.6 Методологія моделювання загроз

В цій роботі використовується методологія моделювання загроз [38], що розроблена саме для автомобілів. Вона сфокусована на виявлені загроз за умови, що зловмисник вже отримав доступ до системи або має можливість здійснити неправомірні дії. Це є доцільним, оскільки далі будуть розглянуті атаки, виконання

яких було практично підтверджено. Згідно з запропонованою методологією моделювання загроз складається з трьох етапів.

Етап 1. Визначення критичного програмного забезпечення (ПЗ) / програмної системи (ПС). Критичними вважаються програми, які швидше за все призведуть до серйозних загроз і тому мають бути досліджені в першу чергу. В межах методології критична програма або система - це функціональність, яка будучи скомпрометованою, може призвести до серйозних наслідків, пов'язаних з безпекою або іншими способами. Далі для всіх ідентифікованих застосувань та систем застосовуються етапи 2 та 3.

Етап 2. Декомпозиція ПЗ / ПС. Цей етап складається з двох кроків. На першому кроці створюються діаграми взаємозв'язків в транспортному засобі (визначаються усі елементи, підсистеми та шини даних, які підключені до розглянутої системи, а також зовнішні з'єднання, такі як Wi-Fi, OBD-II, Bluetooth або стільниковий зв’язок). Другий крок полягає у визначенні високорівневих потоків даних в діаграмі взаємозв’язків

Етап 3. Виявлення та аналіз загроз. Третій крок також складається з двох кроків. Під час першого кроку всі загрози ідентифікуються за допомогою класифікації загроз STRIDE [43]. Це означає, що для кожного ЕКУ, потоку даних та зовнішнього об'єкта по відношенню до мережі використовуються відповідні класи STRIDE для ідентифікації можливих загроз, в результаті чого з'являється список загроз для всіх компонентів системи. Другий крок - це визначення тяжкості загроз. На етапі 3 кожна загроза оцінюється за двома критеріями: строгістю та керованістю. Для визначення строгості (ступеня тяжкості наслідків) загрози використовується класифікація [44]. Класифікація представлена в таблиці 2.2 і дає чітке розмежування між наслідками для одного або декількох транспортних засобів та сфокусована на наступних аспектах: безпека водія; експлуатаційні характеристики автомобіля; приватність даних; фінансові ризики. Стандарт ISO 26262 дає опис вимірювання керованості (таблиця 2.3).

Таблиця 2.2 - Класифікація загроз для визначення ступеня строгості

Рівень	Ступінь впливу на			
	Безпеку водія	Експлуатаційні характеристики автомобіля	Приватність даних водія	Фінансові ризики
1	**2**	**3**	**4**	**5**
0	Жодного впливу	Жодного впливу на експлуатаційні показники	Жодного неавторизованого доступу до даних	Жодних збитків
1	Незначний вплив	Непомітний для водія вплив	Доступ до даних, що не дозволяють ідентифікувати водія або автівки	Незначні збитки (до 10$)

Продовження таблиці 2.2

1	**2**	**3**	**4**	**5**
2	Ризик для життя (з можливістю вижити) або помірні пошкодження для багатьох автомобілів	Водій помічає погіршення експлуатаційних показників або непомітний вплив на декілька автомобілів	Ідентифікація водія або автомобіля або деанонімізовані дані з декількох автомобілів	Помірні збитки (до 100$) або незначні збитки для багатьох автомобілів
3	Ризик для життя (з малою ймовірністю вижити) або суворі пошкодження для багатьох автомобілів	Значний вплив на експлуатаційні показники або помітний вплив на декілька автомобілів	Відстежування водія або автомобіля або ідентифікація багатьох водіїв або автомобілів	Значні збитки (до 1000$) або помірні збитки для багатьох автомобілів
4	Пошкодження з загрозою для життя та фатальними наслідками для багатьох автівок	Значний вплив на чисельні автомобілі	Відстежування багатьох водіїв або автомобілів	Значні збитки для багатьох автомобілів

Таблиця 2.3 - Класифікація загроз за ступеню керованості

Рівень	Опис
0	Повністю контрольована ситуація
1	Легко контролюється водієм
2	Помірно контролюється (більшість водіїв можуть впоратися)
3	Водію важко контролювати ситуацію або непідконтрольне
4	Не може бути контрольованою

Використовуючи значення строгості та керованості, загальний рівень загрози вимірюється наступним чином [44]:

$$T = w_C C \cdot w_S S + w_O O + w_P P + w_F F \quad (2.1)$$

де T – кількісна оцінка загрози;

C – оцінка керованості;

S – оцінка безпеки;

O – оцінка експлуатації;

P – оцінка приватності;

F – оцінка фінансових ризиків;

w_C, w_S, w_O, w_P, w_F – відповідні вагові коефіцієнти, що обираються експертами.

Слід зауважити, що керованість має відношення лише до безпеки, оскільки інші категорії не контролюються водієм повністю або частково, тому значення для безпеки та керованості перемножуються.

2.7 Вибір вагових коефіцієнтів

Кожен з параметрів, що використовується для оцінювання загрози має власний ваговий коефіцієнт. Для обчислення оцінок загроз обираються вагові коефіцієнти для кожного аспекту згідно з пріоритетами при складанні моделі загроз. Вибір конкретних значень робиться експертом або групою експертів.

В даній роботи пріоритетом є безпека і життя водія та пасажирів, а також вплив на експлуатаційні характеристики, оскільки вони також можуть мати вплив на

безпеку водія під час руху. Приватність даних та фінансові ризики мають меншу пріоритетність, оскільки вони не пов’язані з фізичними загрозами для життя людини. З огляду на це, далі використовуються наступні коефіцієнти:

$$w_C = w_S = 10,\ w_O = 7,\ w_P = w_F = 5 \qquad (2.2)$$

2.8 Опис можливих атак

Дослідниками [8] були здійснені атаки з використанням тестового стенду, що складається з реальної автомобільної апаратури. Для цих атак надається детальний опис не тільки наслідків, але й того як проводиться пошук можливості здійснення неавторизованих дій.

Атака на електричний привід вікна. Ця атака передбачає очікування, доки не станеться певна умова (наприклад, швидкість машини перевищує 200 км/год), після чого буде відправлено CAN пакет, що містить код для відкриття вікна водія. Незважаючи на те, що справжній блок управління так само надсилає свої повідомлення з тією ж самою частотою, що показує, що жодна кнопка не була натиснута, вікно відкривається і блокується, поки водій не зреагує, натиснувши кнопку "закрити".

Після ідентифікації повідомлень, що стосуються ініціювання підйому вікна, отримується стратегія нападу, подібна до імітованої атаки: кожен раз, коли відповідний пакет, що містить код, призначений для відкриття вікна, створюється новий пакет із зазначенням протилежної команди, тобто закриття вікна. Цей практичний приклад для сучасного реального автомобіля являє собою атаку відмова від обслуговування на підйомник вікна. Наслідки успішної атаки можуть вплинути як на комфорт (вікно більше не реагує на дії пасажира) та на безпеку (якщо водій не зосереджений на керуванні автомобілем).

Треба враховувати один важливий момент. Оскільки вплив на користувача ПК не може призвести до подальших негативних наслідків, водій, який втратив контроль, може спричинити аварію, навіть за допомогою інших транспортних засобів на дорозі.

Атака на сигнальні лампи. Сигнальні вогні вмикаються системою захисту від крадіжки, коли виявляється вторгнення в припаркований автомобіль. У результаті сигнал тривоги створюється на декілька хвилин, відправляючи команди до ЕКУ відповідального за електроніку автомобіля, щоб встановити або вимкнути попереджувальні вогні. Було виявлено, що кожен компонент із доступом до підмережі, що виконує функції комфорту пасажира, може сильно перешкоджати цьому процесу, негайно відправивши команду вімкнення після того, як була отримана команда ввимкнення (відправлена з підмережі комфорту). Індикаторні лампи залишаються повністю темними майже весь час, лише іноді з'являється коротке, слабке свічення.

Хоча наслідки цієї атаки практично не впливають на комфорт, це може вплинути на безпеку, наприклад якщо вона активізується, поки машина зламана і перешкоджає транспортному засобу вказувати на аварію іншим учасникам дорожнього руху.

Атака на систему управління подушками безпеки. Для цієї атаки модуль управління подушками безпеки був вилучений з системи. Це може бути зроблено зловмисником, який бажає створити загрозу людині в автомобілі (через втрату системи безпеки), але набагато частіше ціллю є гроші. Статистика поліції та преси стверджує, крадіжка систем подушок безпеки досить поширена.

Метою атакуючого є приховування декількох ознак цього видалення, що може рано чи пізно викликати підозру. Це попереджувальна лампа наявності подушок безпеки на приладовій панелі, яка вказує на несправність (або відсутність) системи управління подушкою безпеки або несправність зв'язку з "дефективною" системою за допомогою протоколу діагностики, який може виконуватися в автосервісі після підключення до інтерфейсу діагностики автомобіля.

Щоб контролювати наявність один одного, ЕКУ зазвичай не використовують протокол діагностики, але стежать за іншими повідомленнями, які передаються відповідним компонентом - у цьому випадку модулем керування подушкою безпеки. Один із способів обійти цю перевірку - це видалення системи подушок безпеки з списку пристроїв шлюзу, таким чином він діє так, наче ніколи і не було встановлено

систему подушок безпеки. Більш практичним способом приховування зловмисних дій є визначення повідомлень очікуваних шлюзом від модуля керування подушкою безпеки. Це дозволяє імітувати також загальні повідомлення системи управління подушкою безпеки. Повторно відтворюючи це повідомлення зі очікуваною частотою в підмережі трансмісії, зловмисний пристрій також може імітувати наявність системи подушок безпеки серед інших ЕКУ.

В той час, коли комфорт не страждає (водій не помітить будь-якого недоліку функціональних можливостей при звичайній експлуатації), можливі наслідки для безпеки в надзвичайних ситуаціях можуть бути дуже серйозними.

Атака на систему контролю тиску в шинах. У 2005 році Департамент транспорту США зробив обов'язковим для встановлення у всіх нових автомобілів системи контролю тиску в шинах (Tire Pressure Monitoring System, TPMS). Система TPMS, як правило, складається з передавачів у шинах та приймача всередині автомобіля.

Ця система призначена для попередження аварій, оскільки недокачані або перекачані шини можуть призвести до нещасних випадків. Наприкінці 1990-х років відбулися понад 100 аварій через недокачені шини, що спричинило появу акта TREAD [45] (Transportation Recall Enhancement, Accountability, and Documentation).

Акт TREAD встановлює два правила. Перше вимагає відстеження та відповідь на будь-які можливі ознаки небезпеки з боку транспортного засобу, які потребують реакції водія або створюють ризик для його безпеки. Друге правило передбачає, що всі автомобілі, вироблені в США після 2007 року, повинні включати систему TPMS [45]. Сьогодні повсюдність технології TPMS вважається само собою зрозумілою, створюючи значний ризик, якщо зв'язок між TPMS та ЕКУ буде скомпрометована.

Одним із прикладів зловживання TPMS є відстеження транспортних засобів через унікальний ідентифікатор, що має кожен модуль TPMS. Кожне колесо транспортного засобу, обладнаного TPMS, передає унікальний ідентифікатор, який легко зчитується з використанням приймачів, що не входять в комплект. Це можливо також через те, що канал зв’язку між передавачем на колесі та приймачем

не є зашифрованим [46].

2.9 Загальний алгоритм виконання атаки через мережу CAN

Критичні з точки зору безпеки атаки проти автомобіля складаються з трьох етапів.

Перший етап полягає в тому, що зловмисник отримує доступ до внутрішньої автомобільної мережі. Це дозволяє зловмиснику вводити повідомлення в мережу автомобіля, прямо чи опосередковано контролюючи бажаний ЕКУ. Дослідники з Університету Вашингтона та університету Каліфорнії Сан-Дієго змогли отримати віддалене виконання коду в модулі телематики автомобіля, використовуючи вразливість в програмному забезпеченні Bluetooth-модуля та скомпрометувати стільниковий модем [40].

Кібер-фізичні напади (атаки, що приводять до фізичного контролю різних аспектів автомобіля), з іншого боку, вимагатимуть взаємодії з іншими ЕКУ. Кібер-фізична атака, як правило, вимагає *другого етапу*, який передбачає ін'єкцію повідомлень у внутрішню автомобільну мережу, в спробі взаємодіяти з критично важливими ЕКУ, такими що відповідальні за керування, гальмування, прискорення, тощо.

Третій етап полягає в тому, щоб атакований ЕКУ здійснив певну поведінку, що погіршує безпеку автомобіля. Це передбачає реверс-інженірінг повідомлень у мережі та виявлення точного формату для виконання певних дій.

Підрозділи 2.12 та 2.13 присвячені опису та аналізу атак, що були здійснені по відношенню до автомобілів присутніх на ринку. Це свідчить про те, що здійснення атак на інформаційну безпеку автомобіля не є суто теоретичною можливістю, а може бути практично виконано, особливо при існуючому ставленні виробників транспортних засобів.

Перед описом проаналізованих атак необхідно зазначити, що їх можна поділити за одним критерієм — чи необхідна була діагностична сесія для виконання атаки. За дизайном вона необхідна майстрам з авто центру для виявлення проблем в автомобілі та дозволяє робити операції, що недоступні звичайному користувачу.

Тому неавторизований доступ відкриває значний простір для здійснення атак.

Оскільки відкриття діагностичної сесії зловмисником є зловживанням, то згідно класифікації STRIDE усі атаки, що здійснюються з використання діагностичних пакетів, мають клас "Перевищення привілеїв” (позначається літерою E).

Пакети, що використовуються ЕКУ при звичайних обставинах називаються нормальними. Їх використання зловмисником під час роботи автомобіля не може бути виявлено існуючими методами захисту. Виробники не надають формат пакетів у відкритому доступі, тому зловмисник вимушений спочатку виявити пакети та розібрати формат даних в кожному з них.

2.10 Дерево атаки

Дерево атаки [47] є зручним способом систематично класифікувати різні способи атакувати захищуваний об’єкт. В загальному вигляді атаки на об’єкт представляються в деревоподібній структурі, з ціллю атаки як кореневим вузлом та різними способами досягнення цієї мети як листи дерева. На рисунку 2.2 зображено приклад дерева атаки, де кінцевою ціллю є відкриття сейфа.

Для того, щоб відкрити сейф зловмисник може використати відмички, дізнатися кодову комбінацію, розрізати сейф або скористатися тем, що сейф було встановлено з порушенням вимог. Комбінацію можна знайти записаною або дізнатися від власника і так далі. Кожен вузол, окрім кореневого, є підціллю, а всі підвузли є способами досягнення цієї проміжної цілі.

Вузли можуть бути сполученими або альтернативними. На рисунку усі вузли, де не вказаний тип, є альтернативними вузлами. Сполучені вузли передбачають одночасне виконання умов усіх підвузлів, що можна порівняти з логічним “І”.

Альтернативні вузли вимагають виконання хоча б однієї передумови, що є аналогією логічного “АБО”.

Наступним кроком є визначення для кожного вузла його значення. Наприклад, значення “Можливо” та “Неможливо”. Проте використання

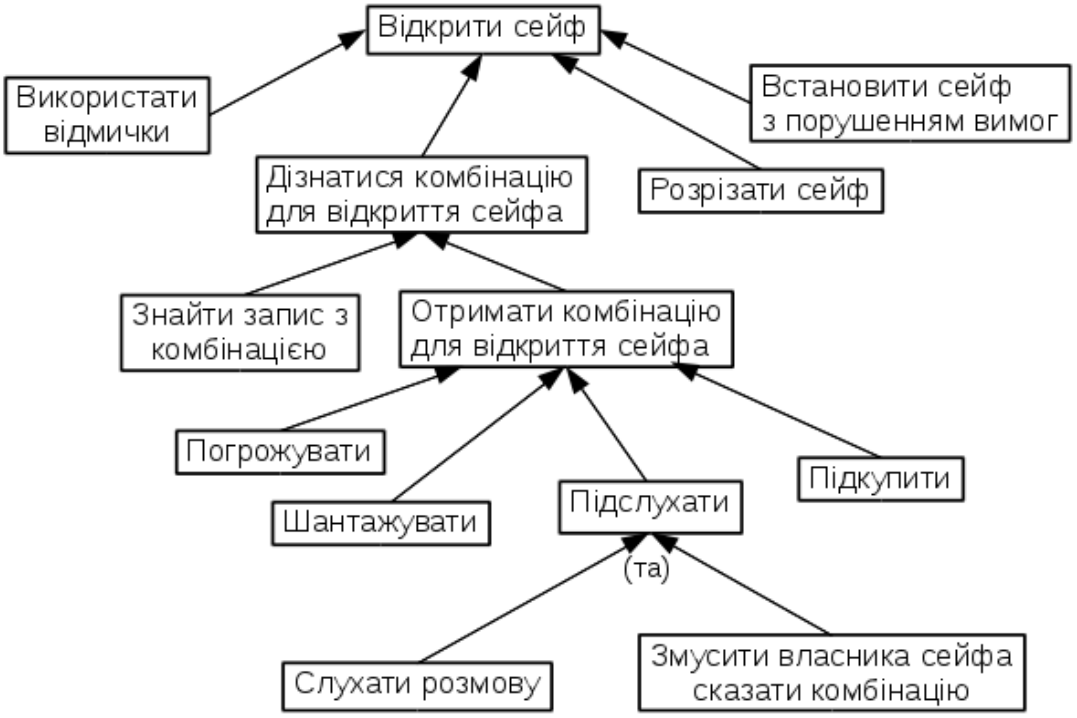

Рисунок 2.2 - Дерево атаки на сейф

кількісних значень надає більше інформації та дозволяє оцінити ймовірність здійснення атаки.

Кожен вузол в дереві атаки є частиною її здійснення і вимагає певних зусиль для здійснення дії, що міститься в вузлі. Шлях від вузлів найнижчого рівня до кореневого визначає послідовність кроків зловмисника для здійснення атаки і сума зусиль кожного кроку можна розглядати як загальні зусилля зловмисника. Очевидно, що зловмисник буде витрачати мінімум зусиль, тобто пройде шляхом, сумарні зусилля якого будуть найменшими.

2.11 Аналіз дерев атак на електронні компоненти управління

У додатку А плакати 2 та 3 містять ілюстрації дерева атаки з використанням нормальних пакетів та дерева атаки з використанням діагностичних команд відповідно. На нижчому рівні в обох деревах знаходиться отримання доступу до мережі, що очевидно є першим кроком для здійснення будь-яких неавторизованих дій. Наступним спільним вузлом є визначення формату даних, який розпізнає цільовий ЕКУ, оскільки неправильно сформовані дані будуть відхилені. Можливість

того, що ЕКУ не здійснює жодних перевірок дійсності вхідних можна вважати замалою.

Для визначення формату даних в обох випадках використовується техніка фазинг, яка полягає в тому, що на вхід програми подаються недійсні, невідповідні або випадково генеровані дані. В даному випадку метою є знаходження тих даних, які ЕКУ сприйме як дійсні.

Для здійснення атаки з використанням діагностичних функцій обов'язковою є відкриття діагностичної сесії, без якої неможливо змусити ЕКУ виконати будь-яку діагностичну функцію. Сесія встановлюється лише після аутентифікації з використанням криптографічного ключа, який, в загальному випадку, унікальний для кожного ЕКУ. Пошук ключа здійснюється повним перебором і може бути отриманий щонайбільше за 7 з половиною діб [34, с.7].

Одним з можливих кроків атаки з використанням нормальних пакетів є зміна прошивки нецільового ЕКУ. Це дозволить здійснювати атаку навіть без встановлення зв'язку з автомобілем, оскільки модифікований ЕКУ сам може здійснювати її, якщо настають певні події, що визначається цілями та мотивацією зловмисника. Процес перепрограмування ЕКУ – це фактично здійснення атаки з використання діагностичних функцій.

2.12 Перелік атак з використанням нормальних пакетів

Атаки, що розглянуті далі, виконані для Ford Escape 2010 та Toyota Prius 2010 [39] і проводились за допомогою нормальних пакетів. Атаки передбачають надсилання пакетів, що формуються та очікуються ЕКУ в мережі автомобіля, тому кожна атака має позначку про клас STRIDE підроблення ідентичності (позначається літерою S).

Показ довільних значень на спідометрі (Форд). Атака дозволяє показати будь-які значення швидкості та обертів двигуна на приладовій панелі.

Показ довільних значень одометра (Форд). Ця атака проводиться так само, як і попередня.

Обмежена можливість керування (Форд). Атака являє собою відмову в

обслуговувані. Цільовим є ЕКУ модуль керування рульовим управлінням (Power Steering Control Module). В результаті здійснення атаки автомобіль не допомагає під час керування, що робить складним поворот колес, а саме неможливо повернути колесо більш, ніж на 45% порівняно з нормальною роботою.

Показ довільних значень на спідометрі (Тойота). Атака проводиться так само, як і для Форда. Пакет з недійсними значеннями швидкості необхідно надсилати безперервно, оскільки оригінальний пакет постійно надсилається.

Спрацювання гальм (Тойота). Атака експлуатує систему передбачення зіткнень (Pre-Collision System), яка допомагає водію уникнути зіткнення з іншим автомобілем. Ця система має можливість змусити автомобіль загальмувати. Здійснення атаки призводить до зменшення швидкості або повного гальмування автомобіля. Результатом атаки є те, що автомобіль буде стояти, навіть якщо натиснути на педаль газу повністю.

Керування автомобілем (Тойота). Тойота має систему Intelligence Park Assist System (IPAS), яка допомагає водію під час паркування. Ця система має можливість змінювати напрямок руху автомобіля, проте лише при швидкості менш, ніж 4 миль/г. Атака полягає в підробці значень від ЕКУ, на дані від яких очікує система IPAS. Атака призводить до можливості повертати на будь-якій швидкості, але ці повороти є доволі різкими, що може спричинити додаткову небезпеку.

Для наступних атак автори роботи [34] не зазначили модель автомобіля з міркувань безпеки:

- *збільшення гучності радіо.*
- *віддалений старт автомобіля.*
- *вимикання двигуна* (атака була виконана на швидкості 40 миль/г, що
- призводить до раптової зупинки).
- *визначення автомобіля* [48] завдяки ідентифікаторам датчиків тиску повітря в шинах (кожен датчик має власний унікальний ідентифікатор).
- *запис розмов в салоні автомобіля* [40] завдяки доступу до вбудованого мікрофона через вразливість в ПЗ модуля телематики.
- *визначення положення автомобіля* [40] завдяки отриманню даних

системи GPS через вразливість в ПЗ модуля телематики.

В таблиці 2.4 наведені числові оцінки строгості та керованості, а також значення загальної оцінки рівня розглянутих атак під час звичайної роботи автомобіля.

Таблиця 2.4 - Значення оцінок строгості і керованості та загальної оцінки рівня атак під час звичайної роботи автомобіля

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Показ довільних значень на спідометрі						
S T	1	0	0	1	1	105
Показ довільних значень одометра (Форд)						
S T	0	0	0	2	0	10
Обмежена можливість керування (Форд)						
D	2	2	0	2	2	424
Показ довільних значень на спідометрі (Тойота)						
S T	1	0	0	1	1	105
Спрацювання гальм (Тойота)						
S T R	2	3	0	3	3	636
Керування автомобілем (Тойота)						
S T R D	3	3	0	3	3	936
Збільшення гучності радіо						
S T	1	0	0	0	1	100
Віддалений старт автомобіля						
S T	0	0	0	3	4	15
Вимикання двигуна						
S T R	4	3	0	3	3	1236
Визначення автомобіля						
I	0	0	3	0	0	15

Продовження таблиці 2.4

1	2	3	4	5	6	7
Запис розмов в салоні автомобіля						
I E	0	0	3	0	0	15
Визначення положення автомобіля						
I E	0	0	3	0	0	15

2.13 Атаки за допомогою діагностичних пакетів

Кожна атака з перелічених нижче здійснюється після встановлення діагностичної ситуації, що є перевищенням привілеїв. Тому кожна атака має відповідний клас в стовпчику для класифікації STRIDE. Опис та результати атак [39] зроблені для Ford Escape 2010 та Toyota Prius 2010.

*Спрацювання гальм (Форд). А*така можлива лише, коли авто припарковано, жодної загрози для життя водія немає. Неможливість розпочати рух унеможливлює найважливішу функцію автомобіля. Після проведення атаки рух стає неможливим, незалежно від того як водій тисне на педаль газу.

Блокування гальм (Форд). Результатом є неможливість зупинити авто при швидкості 5 миль/г та менше. Водій вимушений шукати можливість зупинити шляхом зіткнення з найменшими наслідками для нього та оточуючих автомобілів і людей.

Вимкнення фар та освітлення (Форд). Існує діагностичний пакет який змушує ЕКУ Smart Junction Box вимкнутися. Разом з цим перестають працювати усі пристрої, що залежать від його роботи. Це фари, внутрішнє освітлення, радіо і т. д. Ця атака стає вкрай небезпечною для водія в умовах обмеженої видимості (під час дощу, туману).

Вимикання двигуна (Форд). Вимикання двигуна на довільній швидкості призведе до зупинки шляхом зіткнення. У разі, коли поруч знаходяться інші автомобілі, вони можуть зіткнутися з атакованим автомобілем, що становить загрозу і для їх безпеки.

Вимикання двигуна (Тойота). На відміну від попередньої, ця атака можлива лише, коли автомобіль припаркований, тому вона не становить загрозу для водія.

Вмикання/вимикання гудка (Тойота). Постійний звук гудка зменшує зосередженість водія на ситуації на дорозі, також становить стресову ситуацію, що негативно впливає на здатність адекватно та вчасно реагувати на події під час їзди.

Відкривання /замикання дверей – Тойота. В першу чергу атака забезпечує фізичний доступ до салону та багажника автомобіля. Закриття дверей водієм або пасажиром не допоможе впоратися з атакою, оскільки повторне виконання атаки знову відчинить двері.

Показ довільних значень на індикаторі палива (Тойота). Результатом атаки є те, що водій бачить, що палива вдосталь, хоча воно закінчується. Це може призвести до раптової зупинки під час руху.

Перелік атак [34] для ЕКУ модуль керування тілом (Body Control Module):

– постійна активація реле блокування дверей;

– безперервна робота склоочисників;

– відкриття багажника;

– відміна блокування положення дросельної заслінки (результатом атаки є вплив на дросельну заслінку, яка регулює постачання палива до двигуна і зміна швидкості без дій з боку водія);

– відкриття усіх дверей;

– постійна робота гудка;

– вимикання усього допоміжного освітлення - найбільший ризик атака завдає в умовах обмеженої видимості;

– безперервна подача рідини для склоочисників.

Атаки на ЕКУ модуль керування двигуном [34]:

– тимчасовий приріст кількості обертів двигуна;

– вимикання циліндрів двигуна, рульового управління, гальм – особливістю є те, що водій має можливість скасувати результат атаки (наприклад, завести двигун), що значно збільшує ймовірність того, що водій впорається з ситуацією;

– вимикання двигуна – водій може завести повторно двигун, що зменшує негативні наслідки атаки;

В таблиці 2.5 наведені числові оцінки строгості та керованості, а також значення загальної оцінки рівня розглянутих атак, що можуть мати місце під час діагностики.

Таблиця 2.5 - Значення оцінок строгості і керованості та загальної оцінки рівня атак за допомогою діагностичних пакетів

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Спрацювання гальм (Форд)						
S T R	0	3	0	0	4	15
Блокування гальм (Форд)						
S T R	2	3	0	2	3	631
Вимкнення фар та освітлення (Форд)						
S T R	2	2	0	3	2	429
Вимикання двигуна (Форд)						
S T R	0	3	0	0	4	21
Вмикання/вимикання гудка (Тойота)						
S T R	1	0	0	0	3	300
Відкривання /замикання дверей (Тойота)						
S T R	2	2	0	3	2	429
Показ довільних значень на індикаторі палива (Тойота)						
S T R	2	1	0	3	2	422
Постійна активація реле блокування дверей						
R E	1	2	0	0	1	114

Продовження таблиці 2.5

1	**2**	**3**	**4**	**5**	**6**	**7**
Безперервна робота склоочисників						
R E	1	0	0	0	1	100
Відкриття багажника						

S T E	0	0	0	3	3	15
Відміна блокування положення дросельної заслінки						
R E	2	2	0	0	2	400
Відкриття усіх дверей						
R E	1	2	0	3	2	229
Постійна робота гудка						
S R E	1	0	0	0	1	100
Вимикання усього допоміжного освітлення						
S R E	2	2	0	3	4	829
Безперервна подача рідини для склоочисників						
S R E	2	2	0	3	3	629
Тимчасовий приріст кількості обертів двигуна						
S R E	2	3	0	2	3	631
Вимикання циліндрів двигуна, рульового управління, гальм						
S R E	3	3	0	3	3	921
Збільшення кількості обертів двигуна в режимі спокою						
S R E	2	2	0	2	2	424
Спрацювання гальм для передніх колес						
S R E	3	4	0	4	4	1248
Розблокування гальм, запобігання гальмуванню						
S R E	4	4	0	4	4	1648

Отримані оцінки знаходяться в широкому діапазоні, що свідчить про значну кількість атак, що можуть бути здійснені. Оцінювання загроз дозволяє порівняти загрози між собою та виявити ті, що являють собою найбільшу небезпеку. Ось перелік загроз, що мають найвищі оцінки: розблокування гальм, запобігання гальмуванню (1648); спрацювання гальм для передніх колес (1248); вимикання двигуна (1236). Тоді як найменші оцінки мають показ довільних значень одометра (10); відкриття багажника (15) та загрози, що можуть бути здійснені лише тоді, коли автомобіль припаркований: вимикання двигуна (Тойота) (21) та спрацювання гальм (Форд) (15). Найбільш вплив на оцінку має факт можливості здійснення

неавторизованих дій під час руху автомобіля, чи існує загроза для інших транспортних засобів на дорозі та наскільки важко водію впоратися з наслідками здійснення атаки.

2.14 Поверхня атак ЕКУ

Поверхня атак [49, 50] — це сукупність усіх точок входу (векторів атак) в систему, за допомогою яких неавторизований користувач (зловмисник) може впровадити власні дані, вилучити дані або ініціювати подію, прав на яку він не має. Однією з методик забезпечення безпеки захищуваної системи є утримування поверхні атак в визначених межах.

Поверхня атак визначає, які частини системи потребують перегляду та тестування на наявність вразливостей системи безпеки. Мета аналізу поверхні атаки полягає в тому, щоб зрозуміти зони ризику в захищуваній системі, щоб розробники та спеціалісти з безпеки знали, які частини програми відкриті для атак, могли знайти способи мінімізувати це, і помітити, коли і як поверхня атаки змінюється і що це означає з точки зору оцінки ризиків.

Розділяють поверхні атак для програмного забезпечення, мереж та людську. В залежності від контексту, цей термін має відповідне значення. В даній роботі розглядається поверхня атак для мереж CAN у складі автомобіля.

Перелічені атаки на ЕКУ автомобіля підтверджують наявність вразливостей в існуючих рішеннях, які проектувалися без урахувань інформаційної безпеки. Поверхня атак є інструментом аналітиків, що показує сукупність можливих шляхів здійснення неавторизованих дій по відношенню до захищуваної системи.

Створенням поверхні атак займається група експертів з інформаційної безпеки, які на власний розсуд визначають можливі атаки та надають пріоритети. Також варто зазначити, що більшість робіт з отримання метрик та алгоритму складання поверхні атак зосереджені виключно на системах, які аналізуються. Тобто використання методики, що добре підходить до файлових систем може бути неможливим по відношенню до іншого програмного забезпечення, наприклад ERP систем.

В роботі використовується загальна методика оцінювання поверхні атак [50], яка розрахована на програмне забезпечення, тому необхідно адаптувати її до використання по відношенню до CAN мережі та елементів мережі.

2.15 Методика оцінювання поверхні атаки

Ключовими поняттями в методиці [50] є: канали, сховище даних, методи.

Під *каналом* розуміється будь-який канал зв'язку з мережею, який використовує зловмисник. Це може бути відкритий порт, сокет, підмережа в мережі. Під *сховищем даних* розуміється сукупність даних, які існують постійно або тимчасово. До даних, які зберігаються постійно належать файли, записи бази даних. Тимчасові дані — це дані, що існують в пам'яті процесу, що виконується, тощо. *Методами* є функціональність, яку елемент мережі може виконати. Це може бути реакція на дані, що надійшли з мережі, робота самого елемента мережі згідно з його призначенням, тощо.

Необхідно зазначити, що канали, методи та сховища даних розглядаються як ресурси. Не всі ресурси однаково впливають на оцінку поверхні атак мережі, оскільки не всі ресурси однаково ймовірно будуть використані зловмисником. Внесок ресурсу до поверхні атаки системи залежить від потенціального збитку, тобто рівня шкоди, який зловмисник може заподіяти під час використання ресурсу в атаці та зусиль, які зловмисник витрачає на придбання необхідних прав доступу, щоб мати можливість використовувати ресурс в атаці. Чим вище потенційний збиток або чим менше зусилля, тим вище внесок у поверхню атак.

Оцінювання атак на ЕКУ. Кожен ЕКУ [51] може бути об'єктом декількох атак, кожна з яких спричиняє різні наслідки на функціональність автомобіля, безпеку водія та пасажирів та керування. Одна й та ж сама атака, здійснена по відношенню до двох різних ЕКУ відрізнятиметься в наслідках через те, що кожен ЕКУ відповідає на певну частину функціональності автомобіля. Тому має сенс оцінити саме ЕКУ, а не атаки. Оцінка показуватиме важливість ЕКУ з точки зори безпеки у разі здійснення атак.

Під оцінкою атаки будемо розуміти відношення потенційного збитку до

докладених зусиль [50]:

$$S_{\text{ECU}} = \frac{\sum_{i=1}^{n} T_i}{E_c + E_d + E_m} \tag{2.3}$$

де n- кількість виявлених загроз для оцінюваного ЕКУ;

T_i – оцінка i-ї загрози – величина потенційного збитку (встановлюється експертами з питань інформаційної безпеки автомобіля);

E_c – оцінка зусиль для доступу до каналу, який використовує ЕКУ (експертна оцінка);

E_d – оцінка зусиль для доступу до даних ЕКУ (експертна оцінка);

E_m – оцінка зусиль для виклику методів в ЕКУ (експертна оцінка).

Зусилля, які зловмисник витрачає, наприклад, на відкриття діагностичної сесії можуть дозволити провести йому більше однієї атаки. Тобто зусилля, які були витрачені один раз, дозволяють нанести максимальний збиток в межах отриманого доступу. В такому випадку, зусилля потрібно враховувати лише один раз, тоді як потенційний збиток враховується за кожну атаку. Тож в формулі (2.3) E_c, E_d та E_m - це оцінки унікальних зусиль для виконання усіх атак на розглянутий ЕКУ.

Оцінювання зусиль для доступу до каналів

В роботі [40] показано, що зловмисник може отримати доступ до CAN мереж автомобіля через канали фізичного доступу, канали близької відстані та канали дальньої відстані. Доступ до кожного каналу вимагає від зловмисника різних зусиль та дає різні можливості.

Канали фізичного доступу вимагають безпосередньої взаємодії з обладнанням автомобіля, що може бути ускладнено або неможливо. Також існує загроза того, що зловмисника помітять. Прикладами є OBD-II порт, CD програвач, USB порт, порт підключення мобільного пристрою, пристрій для діагностики.

Канали близької відстані дозволяють зловмиснику отримати доступ, знаходячись поруч без ризику бути поміченим. Приклади: Bluetooth, Wi-Fi.

Канали дальньої відстані дозволяють зловмиснику отримати доступ, знаходячись в будь-якому місці, проте вимагають найбільших зусиль. До каналів дальньої відстані відноситься стільниковий зв’язок.

В рамках роботи вважається що фізичний доступ вимагає найменших зусиль, а доступ через канали дальньої відстані – найбільших зусиль. Таким чином запропоновано таке ранжування значень оцінок:

– оцінка зусиль для фізичного доступу складає $E_{physical} = 1$,

– оцінка зусиль доступу до каналів близької відстані складає $E_{short-range} = 5$,

– оцінка зусиль доступу до каналів дальньої відстані складає $E_{long-range} = 10$.

Очевидно, що зловмисник використає усі можливі канали для здійснення неавторизованих дій. Для обчислення оцінки поверхні атак вважається, що зловмисник використає усі канали зв'язку у спробі здійснити атаку на автомобіль. Для усіх атак оцінка зусиль для доступу до каналів розраховується наступним чином:

$$E_c = E_{physical} + E_{short-range} + E_{long-range} = 16 \quad (2.4)$$

Оцінювання зусиль для доступу до даних

До даних, що представляють інтерес для зловмисника відносяться:

– формат даних, що використовує ЕКУ під час своєї роботи,

– зміст та дійсні значення кожного параметра,

– ключі для здійснення аутентифікації з ЕКУ,

– формат діагностичних команд.

Зловмисник отримує формат даних завдяки зчитуванню пакетів з CAN шини. Ці дані передаються в незашифрованому вигляді. Зміст та значення параметрів зловмисник отримує перебором усіх можливих значень (фазингом) та аналізуючи те, як змінюються значення. Оцінка зусиль для отримання таких даних встановлюється такою: $E_{plaintext} = 1$.

Дані можуть бути зашифровані, що вимагає знання ключа для розшифрування. В такому випадку зусилля для отримання доступу до даних мають наступну оцінку $E_{ciphertext} = 5$

Ключі для здійснення аутентифікації з ЕКУ та діагностичні команди не

передаються під час нормальної роботи ЕКУ, тому зловмиснику необхідно перебирати усі можливі комбінації. Оцінка зусиль для отримання доступу до даних складає $E_{hidden} = 10$.

Для оцінки зусиль для доступу до даних вважається, що зловмисник спробує отримати усі можливі дані, що допоможуть здійснити атаку [39].

Для усіх атак, де використовуються лише нормальні пакети, оцінка зусиль становить

$$E_d = E_{plaintext} = 1 \quad (2.5)$$

Для атак з використанням діагностичних команд зусилля оцінюються як

$$E_d = E_{hidden} = 1 \quad (2.6)$$

Оцінювання зусиль для доступу до методів

З точки зору атакуючого ЕКУ є чорним ящиком, що реагує на дані, що містяться в вхідному пакеті. Простішим способом здійснення атаки є надсилання пакетів, що з'являються в мережі, але з модифікованими значеннями. Далі буде використовуватися термін атака з використанням нормальних пакетів для подібних атак. Оцінка зусиль для доступу до методів в такому випадку складає $E_{unconditional} = 1$.

Деякі ЕКУ вимагають появи певних умов для виконання власних методів. Це може бути очікування зовнішньою події для іншого ЕКУ або спеціальні значення даних, якими ЕКУ володіє. Для виконання таких методів зловмиснику необхідно імітувати пакети від ЕКУ, результати якого очікує цільовий (атакований) компонент. Оцінка зусиль для доступу до методів складає $E_{conditional} = 5$.

Найбільші можливості для здійснення атаки відкривають діагностичні команди, оскільки вони дозволяють зробити те, що недоступно водію під час нормальної роботи. Проте атакуючому необхідно відкрити діагностичну сесію та дізнатися формат діагностичних команд. Оцінка зусиль в такому разі складає $E_{diagnostic} = 10$.

Оцінювання потенційних збитків. В якості оцінок потенційних збитків внаслідок здійснення атаки беруться значення в таблицях 2.4 та 2.5. Оскільки про деякі атаки невідомо які ЕКУ підверглися атаці, то беруться атаки, що були

здійснені проти визначених компонентів.

2.16 Оцінювання поверхні атак для ЕКУ

Оцінка поверхні атак для ЕКУ модуль керування двигуном. Для переліку атак на ЕКУ модуль керування двигуном [34] отримані такі оцінки наслідків здійснення атак (див. таблицю 2.5):

- вимикання двигуна (T =1236);
- вимикання циліндрів двигуна, рульового управління, гальм (T = 921);
- тимчасовий приріст кількості обертів двигуна (T = 631);
- збільшення кількості обертів двигуна в режимі спокою (T =424).

Усі атаки здійснюються з використанням діагностичних пакетів, тому використовуються наступні значення зусиль:

$$E_c = 16, E_d = 10, E_m = 10 \tag{2.7}$$

Оцінка поверхні атак для модуля керування двигуном:

$$s_{ECM} = \frac{631 + 921 + 1236 + 424}{16 + 10 + 10} = 89.2 \tag{2.8}$$

Оцінка поверхні атак для ЕКУ модуль керування тілом. Згідно з [34] наводиться перелік атак на ЕКУ модуль керування тілом (*Body Control Module, BCM*) та оцінки наслідків здійснення цих атак (див. таблицю 2.5) мають такі значення:

- вимикання усього допоміжного освітлення (T = 829);
- безперервна подача рідини для склоочисників (T = 629);
- відміна блокування положення дросельної заслінки (T = 400);
- відкриття усіх дверей (T = 229);
- постійна активація реле блокування дверей (T = 114);
- безперервна робота склоочисників (T = 100);
- постійна робота гудка (T = 100);
- відкриття багажника (T = 15).

Усі атаки здійснені з використанням діагностичних пакетів, тому

використовуються значення зусиль ті ж самі, що і для попереднього ЕКУ. Оцінка поверхні атак для модуля керування тілом:

$$S_{BCM} = \frac{114+100+15+400+229+100+829+629}{16+10+10} = 67.1 \quad (2.9)$$

Оцінка поверхні атак для ЕКУ модуль керування гальмами. Проведення атак на ЕКУ модуль керування гальмами (Electronic Brake Control Module) описано в [34]:

- розблокування гальм, запобігання гальмуванню (T = 1648);
- спрацювання гальм для передніх колес (T = 1248).

Оцінки потенційних наслідків наведені в таблиці 2.5. Атаки також здійснені з використанням діагностичних пакетів і оцінка поверхні атак складає:

$$S_{EBCM} = \frac{1248+1648}{16+10+10} = 80.4 \quad (2.10)$$

Оцінка поверхні атак з використанням нормальних пакетів. Атаки, що здійснюються лише надсиланням пакетів, які передаються під час роботи будь-якого ЕКУ вимагають від зловмисника лише доступу до мережі. Неможливо виділити конкретний ЕКУ для оцінки поверхні атак, оскільки будь-який ЕКУ в мережі є потенційною ціллю зловмисника, тому що він може надіслати через CAN шину пакет усім ЕКУ. Тому наводяться оцінки збитків (див. таблицю 2.4) усіх атак [34, 39, 48], що здійснюються з використанням нормальних пакетів.

- вимикання двигуна (T = 1236);
- керування автомобілем (T = 936);
- спрацювання гальм (T = 636);
- обмежена можливість керування (T = 424);
- показ довільних значень на спідометрі (T = 105);
- показ довільних значень на спідометрі (T = 105);
- збільшення гучності радіо (T = 100);
- віддалений старт автомобіля (T = 15);
- показ довільних значень одометра (T = 10).

Атакуючому потрібно докласти значно менше зусиль для здійснення цих

атак і тому загальна оцінка зусиль також є меншою, ніж для будь-якої атаки, пов’язаної з використанням діагностичних функцій:

$$E_c = 16, E_d = 1, E_m = 1 \quad (2.11)$$

Загальна оцінка для поверхні атак складає:

$$S_{normal} = \frac{105 + 10 + 424 + 105 + 636 + 936 + 100 + 15 + 1236}{16 + 1 + 1} = 198.16 \quad (2.12)$$

Отримана оцінка значно вища, ніж у будь-якої атаки з використанням діагностичних можливостей, що зумовлено значно меншими зусиллями і тим, що враховувались атаки на чисельні ЕКУ, а не один.

Висновок до розділу 2

Даний розділ містить огляд результатів здійснення атак по відношенню до ЕКУ автомобіля. Створена модель загроз за результатами здійснених атак та надані оцінки практично здійсненим атакам з урахуванням наступних критеріїв: безпека водія, вплив на експлуатаційні характеристики автомобіля, приватність даних водія, фінансові ризики та керованість автомобіля. Оцінка залежали від вагових коефіцієнтів, які визначають пріоритети під час оцінювання. Життю водія та його здатності впоратися з наслідками атаки в цій роботі були надані найвищі пріоритети. Як результат, найвищі оцінки отримали атаки, що можуть бути здійснені під час руху автомобіля та ті, що суттєво впливають на можливість водія контролювати рух.

Була адаптована методика оцінювання поверхні атак для програмного забезпечення для застосування до ЕКУ. Запропоновано підхід до кількісного оцінювання поверхні атак, який базується на використанні оцінок величин потенційних збитків від атак та оцінок зусиль для доступу до каналів, даних та методів ЕКУ. Використовуючи цей підхід отримані оцінки атак на ЕКУ, які відображають ступінь суворості наслідків атак.

3 СИСТЕМА ВИЯВЛЕННЯ АТАК ДЛЯ CAN МЕРЕЖІ АВТОМОБІЛЯ

3.1 Аналіз існуючих робіт зі створення СВА для автомобіля

Наявність чисельних атак та можливостей для здійснення неавторизованих дій підтверджують необхідність створення механізмів інформаційної безпеки до яких належить система виявлення атак. Наразі існує невелика кількість робіт [10, 11], які розглядають дизайн та архітектуру систем виявлення атак для автомобіля. Наразі створення таких систем з власними особливостями та вимогами є відкритим питанням.

Очевидно, що кожен водій має власний стиль водіння, який також залежить від типу автомобіля (вантажівка, громадський транспорт, легковий автомобіль, тощо), місцевості (місто, шосе, сільська місцевість) та інших факторів, які неможливо передбачити заздалегідь та використати для побудови профілю користувача. СВА повинна адаптуватися до особливостей поведінки водія і не реагувати на них, як на зловмисні дії. Тому існує необхідність в інструменті, який здатний враховувати індивідуальні особливості пов’язані з водінням.

Апаратне забезпечення автомобіля не має значної обчислювальної потужності, як комп’ютери або смартфони, що накладає обмеження на обчислювальну складність алгоритмів СВА. Також варто зазначити, що програмне забезпечення автомобіля працює як система реального часу [52], що має жорсткі вимоги стосовно швидкодії.

Виявлення неавторизованих дій необхідно в першу чергу для запобігання загрози здоров’ю та життю людей в салоні транспортного засобу і потенційно пасажирів автомобілів поруч з атакованим, тому СВА повинна виявляти та реагувати якомога швидше.

Найбільш близькою до цієї дисертації є робота [10], в якій використовувалась глибинна мережа переконань (ГМП) для виявлення аномалій в даних, що передавалися по шині CAN. ГМП дозволяє скористатися перевагами глибинного

навчання. Наприклад, дослідники отримали результати, в яких багатошаровий перцептрон дає точність в 77% проти 98% у ГМП.

Проте авторами було зроблено припущення, що поле даних кожного пакету містить лише 2 параметри — режим та асоційоване з ним значення. Режим міститься в бітах з індексами від 0 до 20, а значення в бітах з 40 по 60. Ця інформація в подальшому використовувалася для вилучення ознак.

Такі дані є штучними та не схожі на дані, що передаються ЕКУ під час роботи. Кожен ЕКУ має власний формат даних, який визначає які параметри знаходяться в полі даних, їх розмір в байтах або бітах та зміст кожного параметра. Отримані результати не можуть свідчити про ефективність виявлення аномалій, оскільки використана структура даних відрізняється від формату даних, що використовують ЕКУ. Тому для навчання нейронної мережі необхідно чітко визначити формат даних кожного ЕКУ та природу цих даних.

Наприклад, пакет для спідометра Тойоти Пріус [39] має наступний формат: IDH: 00, IDL: B4, Len: 08, Data: 00 00 00 00 CN S1 S2 CS, де IDH та IDL — перші та останні 4 біти ідентифікатора ЕКУ, Len — довжина даних, Data — поле даних, CN — лічильник пакетів, S1 — перший байт значення швидкості, S2 — другий байт значення швидкості, CS — контрольна сума пакету.

А ось формат пакету для системи попередження зіткнень Тойоти Пріус [39]: IDH: 02, IDL: 83, Len: 07, Data: CN 00 S1 S2 ST 00 CS, де IDH та IDL — перші та останні 4 біти ідентифікатора ЕКУ, Len — довжина даних, Data — поле даних, CN — лічильник пакетів, S1 — перший байт значення швидкості, S2 — другий байт значення швидкості, ST — поточний стан автомобіля, який приймає наступні значення: 00 — нормальний стан, 24 — незначні зміни швидкості, 84 — помірні зміни швидкості, 8C — значні зміни швидкості, CS— контрольна сума.

В роботі [11] пропонується СВА, що використовує набір правил для виявлення неавторизованих дій. Використовувались наступні ознаки здійснення атаки:

– невірні значення параметрів для ЕКУ в полі даних;

– створення білого списку дозволених ідентифікаторів ЕКУ, які можуть містить пакети в мережі;

– граничні зміни значення параметра в порівнянні зі значенням в попередньому пакеті;

– визначення частоти надсилання пакетів з певним ідентифікатором.

Всі ці ознаки дійсно дозволяють виявити певні сценарії здійснення атак, проте існують сценарії, які не можна виявити за допомогою зазначених вище правил:

– зловмисник фізично приєднав власне обладнання до ODB-II порту автомобіля для здійснення атаки і використовує дійсні значення параметрів і ідентифікаторів ЕКУ; зловмисник надсилає пакети з очікуваною атакованим ЕКУ частотою;

– зловмисник намагається встановити діагностичну сесію з ЕКУ для здійснення функцій, що необхідні лише для діагностики і надають можливості недоступні для водія;

– зловмисник фізично від’єднав один з компонентів та замінив його власним;

– зловмисник має на меті перепрограмувати ЕКУ.

Досвід розглянутих робіт свідчить про те, що вибір ознак здійснення атак є вкрай важливим для їх виявлення. І це перше з чого варто розпочинати роботу над системою виявлення атак. Проте необхідно брати до уваги те, як працюють ЕКУ і особливості при використанні протоколу CAN.

3.2 Архітектура розробленої системи виявлення атак

В даній роботі описується мережева СВА, що виявляє аномальну поведінку в CAN мережі, в якій працюють ЕКУ автомобіля. Для виявлення аномальної поведінки використовуються штучна нейронна мережа, яка здатна створити профіль водія, навчившись під час водіння.

Система виявлення атак має наступну структуру:

- детектор;
- контекст мережі;
- модуль прийняття рішень;
- база правил;
- система інформування.

Передбачається, що СВА знаходиться в мережі як додатковий ЕКУ, який приєднаний до CAN шини. В якості детектора аномальної поведінки обрано багатошаровий перцептрон, детальний опис якого надано в розділі 3.9.

Детектор очікує появи пакету в мережі та у разі появи передає його до модуля прийняття рішень. Також детектор вимірює сигнал для отримання електричних характеристик, що характеризують ЕКУ, який надіслав пакет.

Контекст мережі — це інформація про поточний стан кожного ЕКУ. Можна вважати, що зберігається зліпок кожного ЕКУ в мережі. Ця інформація необхідна для порівняння даних в пакеті з мережі з тими даними, що ЕКУ отримав безпосередньо до цього пакету.

База правил представлена глибокою мережею переконань, яка зберігає профіль користувача, що представлений ваговими коефіцієнтами нейронів. ГМП навчена нормальній поведінці ЕКУ та аномальній поведінці, тобто атакам.

Модуль прийняття рішень відповідальний за те, щоб перевірити чи не є новий пакет частиною атаки на компонент в мережі. Для цього він отримує інформацію про контекст ЕКУ, який є одержувачем пакету, формує вектор ознак та робить запит до бази правил. У разі якщо нейронна мережа віднесе пакет до одного з класу аномальної поведінки, передається сигнал до системи інформування.

Завданням *системи інформування* є повідомлення інших інформаційних систем автомобіля та водія про можливе здійснення неавторизованих дій. Можливі ситуації, коли не треба повідомляти водія, якщо інші системи автомобіля

підтвердять відсутність зловмисних дій. Наприклад, раптове гальмування автомобіля спричинене водієм є аномальною поведінкою, проте не є зловмисною.

3.3 Моделювання ЕКУ

Для моделювання ЕКУ необхідно визначитися з переліком ознак, що характеризують сам компонент та його поведінку в мережі. Необхідно зазначити, що кожен ЕКУ визначає формат даних, який він сприймає і в разі порушення цього формату пакет ігнорується. Компонент, якому надсилається пакет будемо називати цільовим. Компонент, що відправив пакет — відправником. Варто зазначити, що усі ЕКУ, що можуть надсилати пакети цільовому визначаються виробником на етапі проектування, що також є додатковою інформацією для виявлення атак. Далі наводяться обрані ознаки з детальним описом.

Поле даних. Пакет протоколу CAN містить поле даних, що займає 8 байт. Для створення моделі ЕКУ необхідно мати інформацію про те як і які дані генеруються. По-перше, кожен пакет містить ідентифікатор ЕКУ для якого призначений пакет. Проте відсутній ідентифікатор компонента, що надіслав цей пакет, що є недоліком протоколу CAN. По-друге, формат поля даних є довільним і кожен ЕКУ має власний формат того які дані знаходяться і в якому порядку. Загальний вигляд поля даних описується наступним чином:

$$D = \{P_1, P_2, \dots, P_n, S_1, S_2, \dots, S_2\}, \tag{3.1}$$

де D — поле даних;

n - кількість параметрів;

P_i - значення i-го параметру;

S_i — розмір і-го параметру у бітах.

Пов’язані ЕКУ. Кількість та призначення ЕКУ в мережі CAN автомобіля визначається виключно виробником та не змінюється під час експлуатації транспортного засобу. Можна вважати, що існують лише певні ЕКУ які можуть

надіслати пакети цільовому ЕКУ. І навпаки, кожен ЕКУ повинен отримувати пакети лише від визначених ЕКУ, кількість яких не змінюється. Тому в СВА для кожного ЕКУ реєструються ідентифікатори інших компонентів, які можуть надсилати йому дані. Ці ЕКУ називатимемо пов'язаними з цільовим. Інформація про пов'язані компоненти зберігається в контексті мережі, де також реєструються унікальні електричні характеристики пов'язаних ЕКУ. Під час моделювання для ЕКУ задається множина ідентифікаторів пов'язаних ЕКУ. Якщо ЕКУ необхідні параметри з поля даних від інших ЕКУ, то задається множина, де кожен елемент має наступний формат *Ідентифікатор пов'язаного ЕКУ:Множина параметрів*:

$$\{\{REI_1, P_1^1, P_2^1, \dots, P_{n1}^1\}, \dots, \{REI_n, P_1^n, P_2^n, \dots, P_{nn}^n\}\}, \quad (3.2)$$

де n – кількість пов'язаних ЕКУ;

n_i – кількість параметрів i-го пов'язаного ЕКУ;

REI_i – ідентифікатор i-го пов'язаного ЕКУ;

P_j^i - i-й параметр j–го пов'язаного ЕКУ.

Унікальні електричні характеристики ЕКУ. В якості ознаки, що дозволяє ідентифікувати відправника були запропоновано використовувати його електричні характеристики [8, с.9]. Електронні компоненти виготовляються різними виробниками і виконують різні функції, тому доцільно вважати, що вони мають різні принципові схеми і як результат різні електричні характеристики. Наприклад, рівень сигналу, вихідний опір, тощо.

Це дозволяє виявити компонент встановлений зловмисником в мережу. Недоліком є те, що такий підхід не визначить використання в мережі такого ж компонента, але з модифікованим ПЗ.

Для виробників транспортних засобів буде цікава така ознака також тому, що неофіційне обладнання буде виявлене СВА у разі якщо обрані характеристики відрізняються від тих, що має офіційне обладнання.

Роль у мережі. Деякі ЕКУ приєднані до двох або більше мереж водночас. Такі компоненти називаються шлюзами і вони дозволяють компонентам з однієї мережі надіслати пакет в іншу. Такі ЕКУ – об’єкти підвищеної уваги, тому що скомпрометований шлюз дозволяє атакувати усі ЕКУ в мережах, до яких має доступ шлюз.

Частота надсилання пакетів. Певні ЕКУ надсилають пакети з визначеною та постійною частотою, що визначається під час проектування компонента та змінюється лише з оновленням прошивки. Це може бути фіксований період або певний проміжок часу. Коли зловмисник відправляє пакети для здійснення атаки, це збільшує частоту надсилання пакетів до цільового ЕКУ, що є ознакою здійснення атаки. Також варто зазначити, що частота надсилання є стандартною ознакою виявлення атак у комп’ютерних мережах.

Наявність події необхідної для ЕКУ. Не всі компоненти в мережі працюють незалежно від інших. Деякі використовують інформацію від подій, що з’являється епізодично. Наприклад, гудок або модуль керування вікном спрацьовує лише тоді, коли людина натискає відповідну кнопку або ініціює подію іншим чином. Очевидно, що імітація появи події може призвести до того, що цільовий ЕКУ почне працювати іншим чином та призведе до успішного здійснення атаки. Використання електронних характеристик дозволяє виявити той факт, що обладнання зловмисника надіслало такий пакет. Проте це не дозволить виявити атаку, якщо дані відправляє ЕКУ, де зловмисник має можливість виконати довільний код або ЕКУ з модифікованим ПЗ.

Природа даних. Поле даних містить параметри, формат яких в загальному випадку унікальний для кожного ЕКУ. Кожен параметр має власну природу даних, а саме: неперервні, послідовні та дискретні дані.

Неперервні дані змінюються або в напрямку збільшення, або зменшення, причому значення змінюється поступово, без різких змін значень. Прикладом неперервних даних є кількість обертів двигуна за хвилину.

Послідовні дані характеризуються тим, що значення змінюється з певним кроком. Прикладом послідовних даних є лічильник, який лише збільшується на 1.

Дискретні дані приймають значення лише з скінченої множини можливих значень, наприклад стан в якому працює ЕКУ.

Знання про природу даних дозволяє виявити нетипову зміну значення або недійсне значення.

3.4 Правила генерації даних ЕКУ

Кожен ЕКУ знає власний формат даних та дані, які йому необхідні від інших ЕКУ. Також він має інформацією про те, які значення є дійсними, а які хибними. Для моделювання роботи в мережі ЕКУ має функціонал для генерації як дійсних, так і хибних значень для кожного параметру, що він використовує. Далі наводяться визначення дійсних та хибних даних в межах моделювання.

Дійсні значення — це значення, що виникають під час нормальної поведінки. Вони характеризують роботу ЕКУ згідно з його призначенням.

Дійсним значенням параметра, який містить неперервні значення — є таке значення, що абсолютна різниця між поточним не більше, ніж 5%. В рамках моделювання вважається, що неперервні дані змінюються або в напрямку збільшення до максимального допустимого значення, або в напрямку зменшення до мінімального допустимого. Після того, як значення досягне граничного напрямок зміни значення змінюється на протилежний.

Дійсне значення послідовних даних — це таке, що відрізняється від поточного на значення кроку. Можуть бути накладені обмеження на знак різниці між новим та поточним значенням. Наприклад, лічильник лише збільшується на 1, тому значення, що менше на 1 не є дійсним.

Для дискретних даних дійсним значенням є лише те, що знаходиться в множині допустимих значень. Для моделювання ЕКУ вважається, що параметр приймає послідовно усі значення з множини допустимих значень.

Хибними значеннями є ті, що не відноситься до дійсних і для моделювання атак на ЕКУ необхідно генерувати їх відповідно до природи цих даних.

3.5 Структура вектора ознак для ШНМ

Протокол CAN визначає, що в будь-який момент лише один пакет може бути доступним зчитування з шини і СВА зчитує кожен пакет

Вектор ознак для нейронної мережі містить наступні дані:

– параметри з поля даних; разом зі значенням неперервних та послідовних даних міститься зміна в порівнянні з попереднім значенням у процентах (для неперервних даних) та в абсолютному значенні (для послідовних); попередні значення беруться з контексту мережі;

– вектор унікальних характеристик відправника;

– час між надсиланням попереднього та поточного пакетів від відправника;

– дані про пов’язані ЕКУ, якщо такі є; конкретні дані, що необхідні визначається цільовим ЕКУ.

3.6 Використання нейронної мережі для моделювання роботи ЕКУ

Перелічені ознаки, що характеризують ЕКУ та його роботу дозволяють створити моделі ЕКУ, які значно відрізняються один від одного за ознаками та за принципом роботи. Використання однієї нейронної мережі для навчання нормальній та аномальній поведінці для кожного ЕКУ може вимагати значної кількості нейронів та часу на навчання, проте головною проблемою може стати те, що мережа після навчання даних для одного компонента буде втрачати інформацію про інший.

Тому доцільно описати ознаки та поведінку ЕКУ та для кожного створити ШНМ, яка навчиться моделювати поведінку одного ЕКУ. Як наслідок, СВА матиме ШНМ для кожного ЕКУ в мережі. У разі оновлення прошивки ЕКУ або параметрів

його роботи, то перенавчання доведеться зробити лише для однієї нейронної мережі без впливу на інші. Такий принцип дозволяє створити спеціалізовані мережі з параметрами, що моделюють нормальну поведінку кожного ЕКУ та здатні виявляти здійснення атак з бажаною точністю. Необхідно також зазначити, що це спрощує процес оновлення ПЗ для ЕКУ, оскільки мережа для кожного ЕКУ в ПЗ системи виявлення атак зберігається окремо.

Для того, щоб нейронна мережа була здатна виявити аномальні зміни значень параметрів в полі даних запропоновано використовувати різницю між тим значенням, що вилучено з отриманого пакету і попереднім значенням, що зберігається в контексті системи виявлення атак.

Різниця між попереднім та поточним значеннями необхідна для навчання нейронної мережі того, як змінюється значення кожного параметра та яке значення різниці є допустимим. Різниця залежить від природи даних, для неперервних даних це різниця між поточним та попереднім значеннями, для послідовних це також різниця і додатково значення кроку, для дискретних даних замість різниці передається попереднє значення параметра.

Таким чином під час побудови профілю ЕКУ нейронна мережа буде навчатися не лише тим значенням, які мають параметри під час нормальної поведінки, але й тому яким чином вони змінюються. Це є вкрай важливим для здатності виявити атаки, в яких використовуються дійсні значення з незначними відхиленнями від даних, що надсилає оригінальний ЕКУ.

3.7 Опис модельованих ЕКУ

Були створені 4 моделі ЕКУ для моделювання роботи та генерації даних для навчання ШНМ. Моделі значно відрізняються в параметрах і кожну з низ можна вважати унікальною по відношенню до інших. Таблиці 3.1, 3.3-3.5 містять ознаки та їх значення для моделей ЕКУ 1-4.

Параметр P_1 моделі №1 приймає значення в діапазоні [0-5], природа даних: послідовні, крок (Step) має значення +1 або -1. Параметр P_2 моделі №1 приймає

Таблиця 3.1 – Ознаки моделі №1

Ознака	Значення
Ідентифікатор	$ID = 0x42$
Поле даних	$D = \{P_1, P_2\}$
Ідентифікатори пов'язаних ЕКУ	$AssociatedIDs = \{0x20\}$
Вектори унікальних характеристик пов'язаних ЕКУ	$UniqueFeatures = \{0x20: 0.11, 1.12, 1.9\}$
Пов'язані ЕКУ знаходяться в тій ж самій мережі, що і цільовий	так
Параметри пов'язаних ЕКУ, що необхідні цільовому	$AssociatedECUParams = \{\emptyset\}$
Частота надсилання пакетів для ЕКУ	$F = 200$ мс
Роль у мережі	звичайний компонент

значення в діапазоні [0-60], природа даних: неперервні. При значенні $P_1 = 0$, крок має значення +1, при значенні 5 крок дорівнює -1, для всіх інших значень параметра P_1 крок може приймати значення +1 або -1. Дійсні значення параметра P_2 залежать від значення P_1, що представлено в таблиці 3.2.

Для цієї моделі формується наступний вектор ознак для навчання нейронної мережі:

$$\{0x42, P_1, \Delta_1, S, P_2, \Delta_2, 0x20, 0.11, 1.12, 1.9, T\},$$

де Δ_1 — різниця між попереднім значенням параметру P_1 і вилученим з пакета;

S — значення кроку при поточному значенні параметра P1;

Δ_2 — різниця між попереднім значенням параметру P2 і вилученим з пакета.

Таблиця 3.2 – Залежність значень параметрів моделі №1

Параметр P_1	Параметр P_2
0	0-9
1	10-19
2	20-29
3	30-39
4	40-49
5	50-60

T — час між отриманням попереднього пакета для даного ЕКУ.

Розмірність вектора ознак складає 11.

Параметри P_1 та P_2 моделі №2 не залежать один від одного. Параметр P_1 представлений неперервними даними, діапазон допустимих значень [0-1000]. Параметр P_2 представлений неперервними даними, діапазон допустимих значень [0-100]. Для цієї моделі формується наступний вектор ознак для навчання нейронної мережі:

$$\{0x19, P_1, \Delta_1, P_2, \Delta_2, 0x20, 0.2, 1.8, 1.5, 0x86, 0.3, 1.4, 2.1, T\}$$

де Δ_1 — різниця між попереднім значенням параметру P1 і вилученим з пакета;

Δ_2 — різниця між попереднім значенням параметру P2 і вилученим з пакета;

T — час між отриманням попереднього пакета для даного ЕКУ;

Розмірність вектора ознак складає 14.

Параметри P_1, P_2, P_3 моделі №3 не залежать один від одного. Параметр P_1 представлений неперервними даними, діапазон змін = [0-128]. Параметр P_2

Таблиця 3.3 – Ознаки моделі №2

Ознака	Значення
Ідентифікатор	$ID = 0x19$
Поле даних	$D = \{P_1, P_2\}$
Ідентифікатори пов'язаних ЕКУ	$AssociatedIDs = \{0x20, 0x86\}$
Вектори унікальних характеристик пов'язаних ЕКУ	$UniqueFeatures = \begin{Bmatrix}\{0x20: 0.2; 1.8; 1.5\},\\ \{0x86: 0.3; 1.4; 2.1\}\end{Bmatrix}$
Пов'язані ЕКУ знаходяться в тій ж самій мережі, що і цільовий	так
Параметри пов'язаних ЕКУ, що необхідні цільовому	$AssociatedECUParams = \{\emptyset\}$
Частота надсилання пакетів для ЕКУ	$F_{0x20} = 100$ мс для пакетів від ЕКУ з ідентифікатором 0x20, $F_{0x86} = 250$ мс для пакетів від ЕКУ з ідентифікатором 0x86
Роль у мережі	звичайний компонент

представлений дискретними даними, діапазон допустимих значень = [0, 3, 20, 85]. Параметр P_3 представлений послідовними даними з кроком +1, діапазон допустимих значень [0-64], після досягнення максимального значення наступним значенням є 0.

Пакети для цього ЕКУ надсилаються не періодично за наступною схемою: кожні 2000 мс генеруються 10 пакетів з дійсними значеннями і надсилаються з періодом в 50 мс.

Для моделі №3 формується наступний вектор ознак:

$$\{0\text{x}55, P_1, \Delta_1, P_2, P_{2\,prev}, P_3, \Delta_3, S, 0\text{x}44, 0.16, 1.3, 1.8, T\}$$

Таблиця 3.4 – Ознаки моделі №3

Ознака	Значення
Ідентифікатор	$ID = 0x55$
Поле даних	$D = \{P_1, P_2, P_3\}$
Ідентифікатори пов'язаних ЕКУ	$AssociatedIDs = 0x44$
Вектори унікальних характеристик пов'язаних ЕКУ	$UniqueFeatures = \{0\text{x}44: 0.16; 1.3; 1.8\}$
Пов'язані ЕКУ знаходяться в тій ж самій мережі, що і цільовий	так
Параметри пов'язаних ЕКУ, що необхідні цільовому	$AssociatedECUParams = \{\emptyset\}$
Частота надсилання пакетів для ЕКУ	ні
Роль у мережі	звичайний компонент

де Δ_1 — різниця між попереднім значенням параметру P1 і вилученим з пакета;

$P_{2\,prev}$ — попереднє значення параметру P2;

Δ_3 - різниця між попереднім значенням параметру P3 і вилученим з пакета;

S - значення кроку при поточному значенні параметра P1;

T — час між отриманням попереднього пакета для даного ЕКУ.

Вектор ознак має розмір 12.

Параметр P_1 моделі №4 приймає дискретні значення з множини [1, 2] в залежності від значень параметра P_2. Параметр P_2 приймає дискретні значення з множини {0x08, 0x13, 0x25, 0x45, 0x55}, тобто один з ідентифікаторів пов'язаних ЕКУ. Параметр P_3 приймає значення неперервні значення [0-255].

Таблиця 3.5 – Ознаки моделі №4

Ознака	Значення
Ідентифікатор	$ID = 0x70$
Поле даних	$D = \{P_1, P_2, P_3\}$
Ідентифікатори пов'язаних ЕКУ	$AssociatedIDs =$ $\{0\text{x}08, 0\text{x}13, 0\text{x}25, 0\text{x}45, 0\text{x}55\}$
Вектори унікальних характеристик пов'язаних ЕКУ	$UniqueFeatures = \begin{Bmatrix} \{0\text{x}08: 0.9; 1.2; 2.0\}, \\ \{0\text{x}13: 1.2;\ 3.0;\ 2.3\}, \\ \{0\text{x}25: 0.4;\ 2.1;\ 1.8\}, \\ \{0\text{x}45: 2.0;\ 3.8;\ 1.1\}, \\ \{0\text{x}55: 1.0;\ 2.2;\ 3.3\} \end{Bmatrix}$
Пов'язані ЕКУ знаходяться в тій ж самій мережі, що і цільовий	ні ЕКУ з ідентифікаторами 0x08 та 0x13 знаходяться в мережі 1, а ЕКУ з ідентифікаторами 0x45 та 0x55 в мережі 2
Параметри пов'язаних ЕКУ, що необхідні цільовому	$AssociatedECUParams = \{\emptyset\}$
Частота надсилання пакетів для ЕКУ	ні
Роль у мережі	шлюз

Для цієї моделі формується наступний вектор ознак:

$$0\text{x}70, P_1, P_{1prev}, P_2, P_{2prev}, P_3, \Delta_3, 0.9, 1.2, 2.0, 1.2, 3.0, 2.3,$$

$$0.4, 2.1, 1.8, 2.0, 3.8, 1.1, 1.0, 2.2, 3.3, T$$

де P_{1prev} — попереднє значення параметру P_1;

P_{2prev} — попереднє значення параметру P_2;

Δ_3 - різниця між попереднім значенням параметру P_3 і вилученим з пакета;

T — час між отриманням попереднього пакета для даного ЕКУ.

Вектор ознак для цієї моделі має розмірність 23.

Описані моделі, їх параметри, ознаки та нормальна поведінка є представленням реальних ЕКУ на основі інформації про здійснені атаки [34, 39, 40, 46, 48]. Ці моделі будуть використані в розділі 3.10 для опису моделювання роботи ЕКУ в мережі та генерації пакетів для навчання та тренування нейронної мережі.

3.8 Ознаки нормальної та аномальної поведінки ЕКУ в мережі

Для коректної роботи СВА та навчання ГМП необхідно визначити, що є нормальною поведінкою для зменшення хибно позитивних виявлень атак. В той же час важливо детально описати відомі атаки, щоб нейронна мережа навчилася виявляти їх як аномальну поведінку.

Нормальна поведінка — це ті дані, які генерують ЕКУ під час свого функціонування згідно з тим, як заплановано виробником транспортного засобу. Пакети, що генеруються в цьому режимі називаються нормальними. Значення параметрів в полі даних є дійсними; значення змінюються дійсним чином; ЕКУ надсилають пакети з визначеною частотою або лише у разі появи відповідної події; ЕКУ отримує пакети лише від тих компонентів, що можуть надсилати йому і так далі.

Нормальною поведінкою вважається рух та зупинка автомобіля без різких змін швидкості, прискорення, напрямку руху, інтенсивного використання будь-якої функціональності.

Далі наводиться класифікація атак та алгоритми їх здійснення.

Атака відмова в обслуговуванні. Ця атака здійснюється шляхом постійного надсилання пакетів з ідентифікатором цільового ЕКУ з тими даними, які необхідні зловмиснику. Дані можуть містити як дійсні, так і хибні значення.

Ознакою цієї атаки є висока частота надсилання пакетів з ідентифікатором одного й того ж ЕКУ. Під час цієї атаки частота значно вища, ніж під час нормальної роботи.

Алгоритм моделювання атаки:

Крок 1. Генеруються пакети з частотою в 10 разів більше, ніж очікує цільовий ЕКУ. Значення можуть бути дійсними або хибними по відношенню до оригінальних даних.

Крок 2. Згенеровані пакети надсилаються одразу ж після генерації. Оригінальні дані надсилаються з очікуваною частотою. Оскільки вони передаються разом з пакетами зловмисника, то порушується вимоги стосовно частоти надсилання пакетів до цільового ЕКУ.

Атака з використанням нормальних пакетів. Пакети для здійснення атаки можуть містити дійсні значення і тому перевірка даних в пакеті не може гарантувати визначення того, що їх надсилає зловмисник. Передбачається, що зловмисник фізично приєднав власне обладнання для здійснення атаки.

Атака може проводитися наступними способами:

– надсилаються пакети для цільового ЕКУ з дійсними значеннями.

– надсилаються пакети з ідентифікатором ЕКУ, який пов’язаний з цільовим.

– надсилаються пакети з ідентифікаторами цільового ЕКУ та пов’язаних з цільовим.

Для способу 3 пропонується назва композиційна атака, оскільки вона є одночасним здійсненням атаки з використанням нормальних пакетів по відношенню до 2 або більше ЕКУ.

Атака має наступні ознаки:

– значення даних в пакеті, що відрізняються від тих, що надсилалися до здійснення атаки;

– збільшена частота надсилання пакетів з ідентифікатором атакованого ЕКУ. Мережею одночасно передаються і пакети для здійснення атаки, і оригінальні. Для ЕКУ, що надсилають свої пакети не періодично ця ознака не працює.

Лише певні ЕКУ надсилають пакети до цільового при нормальній поведінці. Використання унікальних характеристик ЕКУ виявляє пакети, що надіслані непов’язаним компонентом.

Алгоритм моделювання атаки з використанням нормальних пакетів

Крок 1. Пакети генеруються та надсилаються з очікуваною для ЕКУ частотою. Мається на увазі частота надсилання зловмисних пакетів. У разі, якщо моделюється обладнання зловмисника вектор унікальних характеристик відрізняється від тих, що мають пов’язані ЕКУ. Значення параметрів в полі даних можуть бути дійсними або хибними по відношенню до оригінальних даних.

Крок 2. Оригінальні дані надсилаються з очікуваною для цільового ЕКУ частотою.

Атака з використанням діагностичних команд. Автомобільними виробниками закладено в ЕКУ додаткові функції, що необхідні під час діагностики в сервісному центрі. Передбачається, що лише авторизовані працівники мають доступ до них, проте зловмисник може отримати доступ до цієї функціональності. Спершу необхідно відкрити діагностичну сесію за допомогою криптографічного ключа (для кожного ЕКУ свій). Потім надсилаються пакети з діагностичними командами та параметрами.

В реалізованій СВА відкриття діагностичної сесії або надсилання діагностичних пакетів заборонено. Передбачається, що автомеханік повинен фізично вилучити ЕКУ з СВА від мережі автомобіля, щоб здійснити діагностику.

Для моделювання обрано один формат даних для відкриття діагностичної сесії та для виконання діагностичної команди для усіх ЕКУ.

Алгоритм моделювання атаки з використанням діагностичних команд

Крок 1. Мережею надсилається пакет для здійснення аутентифікації перед створенням діагностичної сесії. Значення в полі даних не має значення.

Крок 2. Мережею надсилається пакет для виконання діагностичної команди. Значення в полі даних не має значення.

Атака, що здійснюються ЕКУ з модифікованим ПЗ. Ця атака передбачає, що зловмисник зміг змінити ПЗ в ЕКУ на модифіковане. В такому випадку зловмиснику не треба встановлювати в мережу додатково своє обладнання, що потім виявляється через підвищену частоту повідомлень. Модифікований ЕКУ може навіть зберігати приблизно ту ж саму частоту надсилання пакетів, проте його робота повинна відрізнятися від нормальної поведінки, інакше ніякої атаки не здійснюється.

Відмінність в роботі модифікованого ЕКУ від роботи ЕКУ з оригінальним ПЗ і є головною ознакою здійснення атаки. Нейронна мережа, що навчена нормальній поведінці ЕКУ в мережі, здатна виявити аномальну поведінку модифікованого ЕКУ. Для моделювання атаки вважається, що скомпрометований ЕКУ є пов’язаним з цільовим.

Алгоритм моделювання атаки , що здійснюються ЕКУ з модифікованим ПЗ

Крок 1. Пакети генеруються з очікуваною цільовим ЕКУ частотою. Поле даних містить дійсні значення, що згенеровані для нормальної роботи.

Крок 2. Значення кожного параметру поля даних є дійсним з точки зору допустимих значень, проте вони відрізняються від тих, що надсилаються під час

нормальної поведінки. Для імітації здійснення атаки пропонується відтворення раніше надісланих пакетів у зворотній послідовності.

Невідомі атаки. Система виявлення може знаходити лише ті атаки, які були відомі під час її розробки. Проте завжди існує ймовірність, що в мережі буде здійснена атака, яку раніше не виявляли. Останній клас атак необхідний для того, щоб позначити ним усю аномальну поведінку в мережі під час роботи СВА. Варто зазначити, що це не обов'язково зловмисна діяльність. Наприклад, водій, що раптово загальмував перед собакою, що вибіг перед машиною. Ця поведінка є доволі нетиповою, проте не пов'язаною зі здійсненням атаки на ЕКУ автомобіля.

Алгоритм моделювання невідомої атаки

Крок 1. Пакети генеруються з частотою, що відрізняються від очікуваної на 5-15%. Частота обирається один раз для моделювання атаки.

Крок 2. Дані параметру містять хибні значення в залежності від природи даних.

Крок 3. Після генерації оригінального пакету він передається мережею з очікуваною частотою ще n разів. Точна кількість надсилань може бути фіксованою під час усіх моделювань здійснення атаки або змінною для кожного окремого моделювання.

3.9 Архітектура багатошарового перцептрону

В даній роботі використовується багатошаровий перцептрон (БШП) з 4 шарами, кожен з яких має меншу по відношенню до попереднього розмірність та свої функції активації. Розмір вибірки для навчання складає 128 векторів, оскільки більші значення не дають збільшення точності результатів. Характеристики шарів БШП перелічені в таблиці 3.6. В якості функції втрат використовується середньоквадратична похибка. Загальна архітектура БШП зображена на плакаті 5 додатку А.

Оскільки найбільша розмірність серед усіх векторів ознак дорівнює 23, то перший шар має таку розмірність. У разі коли довжина вектора ознак менше, ніж 23, то до вектора ознак дописується така кількість нулів, щоб утворений вектор мав розмірність 23.

Перший шар має функцію активації гіперболічний тангенс, що використовується для нормалізації вхідних даних. Другий та третій шари

Таблиця 3.6 – Характеристики шарів БШП

Номер шару	Функція активації	Розмірність вхідних даних
1	Гіперболічний тангенс	23
2	Випрямляч (rectified linear unit)	16
3	Випрямляч (rectified linear unit)	10
4	Нормована експоненційна функція (функція Softmax)	6

використовують функцію активації ReLU (випрямляч) [53]. Ця функція набула популярності для використання в нейронних мережах через те, що її обчислення відбувається швидше, ніж для сігмоїди та гіперболічного тангенсу і тому, що ReLU підвищує збіжність стохастичного градієнтного спуску порівняно з сігмоїдою та гіперболічним тангенсом. Також ця функція відрізняється відсутністю насичення.

Розмірність кожного шару перцептрону є меншою, ніж у попереднього, що необхідно для зменшення розмірності даних та вилучення більше деталізованих ознак в порівнянні з попереднім шаром. Оскільки усі пакети належать до 6 класів, що відповідають нормальній поведінці та 5 типам аномальної поведінки, то вихідний шар має розмірність 6.

В якості функції активації вихідного шару використовується функція Softmax, яка є узагальненням логістичної функції, що нормує n-вимірний вектор із довільним значеннями компонент до n-вимірного вектора з дійсними значеннями компонент в області [0, 1] що в сумі дають одиницю. В даному випадку функція Softmax використовується для багатокласової класифікації.

3.10 Моделювання роботи ЕКУ в мережі

Наступним кроком є генерація даних для ЕКУ згідно з їх нормальною поведінкою та проведення усіх типів атак для отримання даних, що будуть використані для навчання багатошарового перцептрона. Для кожної моделі ЕКУ, що описані в розділі 3.7, генеруються дійсні дані та ті, що відносяться до наступних типів атак:

- атака відмова в обслуговуванні;
- атака з використанням діагностичних функцій;
- атака з використанням нормальних пакетів;
- атака з використанням скомпрометованого ЕКУ;
- невідома атака;

З кожного генерованого пакета отримується вектор ознак для ШНМ. Для навчання була обрана кількість 60000 векторів, по 10000 на кожен клас, який повинна виявляти мережа. Для тренування мережі були отримані 6000 векторів ознак.

Для генерації даних для навчання були обрані початкові значення для кожної моделі ЕКУ, які після цього змінювалися за правилами, що надані в розділі 3.7. Так само були обрані початкові значення для генерації даних для тренування, проте з іншими значеннями, щоб уникнути ситуації перенавчання [2]. В таблицях 3.7 – 3.10 наводяться обрані значення.

Процес навчання нейронної мережі є досить чутливим до даних, які надаються мережі та порядку їх появи. Деякі атаки, наприклад відмова в обслуговуванні, полягають в передачі послідовності пакетів, тому під час навчання збережено цю особливість і мережа отримує до 10 пакетів, що відповідають певній атаці.

Таблиця 3.7 – початкові значення параметрів моделі ЕКУ №1

Параметр / Фаза	P_1	Крок параметра P_1	P_2
Навчання	1	+1	12
Тренування	3	-1	33

Таблиця 3.8 – Початкові значення параметрів моделі №2

Параметр / Фаза	P_1	Напрямок зміни параметра P_1	P_2	Напрямок зміни параметра P_2
Навчання	700	В напрямку збільшення	20	В напрямку збільшення
Тренування	310	В напрямку зменшення	55	В напрямку зменшення

Таблиця 3.9 – початкові значення параметрів моделі ЕКУ №3

Параметр / Фаза	P_1	Напрямок зміни параметра P_1	Параметр P_2	Параметр P_3	Крок параметру P_3
Навчання	40	В напрямку збільшення	0	10	+2
Тренування	88	В напрямку зменшення	20	26	+2

Таблиця 3.10 – початкові значення параметрів моделі ЕКУ №4

Параметр / Фаза	Параметр P_1	Параметр P_2	Параметр P_3	Напрямок зміни параметра P_3
Навчання	1	0x13	90	В напрямку зменшення
Тренування	2	0x45	128	В напрямку збільшення

3.11 Результати виявлення аномальної поведінки

Практичне застосування показало, що точність виявлення поведінки залежить від складності та обсягу даних, що використовує ЕКУ та типу атаки. Виявлення невідомої атаки має найгірші показники через те, що ця атака є схожою до нормальної поведінки ЕКУ. Обраний алгоритм моделювання фактично є нормальною поведінкою з модифікованими параметрами, проте цей клас додано для того, щоб позначити ним будь-які нетипові події, що не схожі з відомими типами атак. Лише модель ЕКУ №4 має високі показники виявлення цієї атаки через те, що два параметри приймають лише дискретні значення, що значно спрощує виявлення.

Найкраще виявляються атаки відмова в обслуговуванні, атаки з використанням діагностичних функцій та атаки, здійснені скомпрометованим ЕКУ, оскільки вони мають чіткі ознаки, які не змінюються в залежності від даних. Це різниця в часі між надсиланнями пакетів, коди діагностичних команд та унікальні електричні характеристики, що відрізняються від очікуваних.

Результати виявлення нормальної та аномальної поведінки для кожної моделі ЕКУ наведені в таблицях 3.11 – 3.14. Результатом є відношення правильної класифікації пакета, що належить до певної поведінки до загальної кількості таких пакетів.

Таблиця 3.11 – Результати виявлення поведінки моделі ЕКУ №1

Нормальна поведінка	86%
Атака відмова в обслуговуванні	93%
Атака з використанням діагностичних функцій	100%
Атака з використанням нормальних пакетів	71%
Атака з використанням скомпрометованого ЕКУ	60%
Невідома атака	48%

Таблиця 3.12 – Результати виявлення поведінки моделі ЕКУ №2

Нормальна поведінка	75%
Атака відмова в обслуговуванні	94%
Атака з використанням діагностичних функцій	100%
Атака з використанням нормальних пакетів	70%
Атака з використанням скомпрометованого ЕКУ	53%
Невідома атака	42%

Таблиця 3.13 – Результати виявлення поведінки моделі ЕКУ №3

Нормальна поведінка	71%
Атака відмова в обслуговуванні	83%
Атака з використанням діагностичних функцій	100%
Атака з використанням нормальних пакетів	72%
Атака з використанням скомпрометованого ЕКУ	68%
Невідома атака	53%

Таблиця 3.14 – Результати виявлення поведінки моделі ЕКУ №4

Нормальна поведінка	88%
Атака відмова в обслуговуванні	75%
Атака з використанням діагностичних функцій	100%
Атака з використанням нормальних пакетів	85%
Атака з використанням скомпрометованого ЕКУ	71%
Невідома атака	90%

Висновок до розділу 3

Основним результатом цього розділу є надання ознак для моделювання ЕКУ, того, як ознаки пов’язані з роботою компонентів та приклади моделювання ЕКУ за допомогою визначених ознак. Був наданий опис того які дані вважити дійсними в залежності від природи даних та які хибними. Надані алгоритми здійснення чотирьох відомих атак та ознаки того, що вважати невідомою атакою. Все це дозволяє описати роботу реальних ЕКУ для побудови їх моделі та створення бази правил для системи виявлення атак. Тобто отримані результати не обмежені виключно використанням у складі СВА або застосуванням ШНМ в якості детектора аномалій.

Були створені чотири моделі ЕКУ, що значно відрізняються між собою для моделювання компонентів з принципово різною нормальною поведінкою, запропоновано архітектуру багатошарового перцептрона для класифікації пакетів для ЕКУ.

За результатами навчання БШП зроблені наступні висновки: атака з використанням нормальних пакетів представляє широкий діапазон можливих атак, що ускладнює виявлення цих атак і існує потреба в розбитті цього класу аномальної поведінки на сукупність менш загальних класів. Клас невідома атака, що повинен відображати всі події, які не відносяться до нормальної та відомої аномальної

поведінки також є занадто загальним, що не дозволяє ефективно виявляти такі атаки. Пропонується виділити більш конкретні класи для навчання БШП для збільшення показника виявлень.

4 ОПИС ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СИСТЕМИ

4.1 Вимоги до розробки програмного продукту

Для виконання завдань даної роботи було розроблено програмне забезпечення (ПЗ) для моделювання ЕКУ та генерації даних для них, моделювання роботи ЕКУ в мережі, навчання і тренування багатошарового перцептрону та демонстрації роботи системи виявлення атак. Для процесу розробки були висунуті наступні вимоги:

– все програмне забезпечення повинно бути написано однією мовою програмування для ефективної інтеграції програмних продуктів;

– оскільки основною метою є демонстрація застосування теоретичних результатів обрана мова програмування повинна дозволяти швидко створювати пз та мати низький поріг входу;

– повинні існувати ефективні та перевірені програмні продукти (бібліотеки, фреймворки, тощо), що мають прикладний програмний інтерфейс для обраної мови програмування.

Для розробки програмного забезпечення було обрано мову Python [54], як ту, що задовольняє усім вищеозначеним вимогам. Python є скрипковою мовою, що дозволяє писати однаковий за функціональністю, проте менший за кількістю рядків код в порівняні з іншими популярними мовами програмування. В той же час Python дозволяє вирішувати широкий спектр задач, що обумовило його популярність. Розроблене ПЗ виконувалось в операційній системі Linux (дистрибутив Debian 9.0) за допомогою командного рядку Bash. Під час розробки використовувались наступні фреймворки.

Python-can – ця бібліотека [55] надає можливість використовувати протокол CAN для генерації та обміну даних, має абстракції для роботи з чисельним апаратним забезпеченням та пропонує набір функцій, що спрощують роботу з пристроями, які використовують CAN. До переваг також відноситься зручне встановлення у разі використання ОС Linux, де на відміну від Windows непотрібно встановлювати чисельні пакети залежностей. Важливим виявилося те, що ця

бібліотека дозволяє працювати з віртуальною шиною CAN без додаткових зусиль, що є вкрай зручним за відсутності апаратного забезпечення.

NumPy – це пакет для наукових обчислень [56], що набув значної популярності в спільноті науковців. Фреймворк надає реалізацію чисельних математичних методів та алгоритмів у сфері обробки сигналів, машинного навчання, сортування, лінійної алгебри і т.д. До того ж існують багато функцій та модулів, що значно спрощують обчислення та роботу з математичним апаратом. NumPy поширюється як програмне забезпечення з відкритим кодом та вільним доступом і позиціонується як альтернатива пакету прикладних програм MATLAB.

TensorFlow — бібліотека з відкритим кодом для машинного навчання [57], яка розроблена компанією Google для задоволення її внутрішніх потреб у системах, здатних будувати та тренувати нейронні. Перевагами цього фреймворку є висока якість коду, оскільки компанія Google використовує його у власних комерційних рішеннях, можливість виконувати обчислення на декількох обчислюваних блоках (центральний або графічний процесор), доступність на усіх популярних операційних системах (Linux, macOS, Windows включно з Android та iOS).

Keras – це високорівневий прикладний програмний інтерфейс для роботи з нейронними мережами [58], що абстрагує взаємодію з бібліотеками для машинного навчання, наприклад, TensorFlow, CNTK, Theano. Основною метою є надання користувачу можливості швидко та максимально просто розпочати роботу над створенням нейронної мережі без необхідності враховувати усі вимоги спеціалізованих бібліотек. Взаємодія з бібліотекою TensorFlow відбувалась за допомогою Keras.

4.2 Структура програмного продукту

Розроблене програмне забезпечення складається з двох основних частин:

- модуль моделювання ЕКУ;
- система виявлення атак.

Модуль моделювання ЕКУ. До функціоналу модуля відносяться створення та зберігання об’єктів, що представляють модельовані електронні компоненти управління, створення об’єкті, що містять логіку кожної атаки та генерують дані відповідно до нормальної роботи ЕКУ, генерація даних, що належить до усіх класів, які повинен виявляти БШП.

Був створений загальний клас ECU для представлення електронного компонента управління. Він отримує ознаки ЕКУ (див. підрозділ 3.3) під час ініціалізації та має метод, який повинні реалізувати усі дочірні класі - *generateValidData(delta)*;

Метод отримує вхідний параметр, що містить різницю в часі між поточним та останнім викликом методу того ЕКУ, який використовується. Він призначений для генерації даних, що відповідають нормальній роботі.

Для кожного типу атак створюється відповідній об’єкт класу, що наслідує базовий клас *Attack*. Це класи *DosAttack, NormalPacketsAttack, DiagnosticPacketsAttack, CompromisedECUAttack, UnknownAttack*. Кожен з них містить логіку того, як саме здійснити атаку з використанням інформації про ЕКУ та дані, що нормальними на момент імітації здійснення атаки.

Модуль моделювання отримує об’єкт моделі ЕКУ та імітує роботу ЕКУ в мережі разом зі здійсненням атак. Модуль моделювання використовує лічильник, що позначає пройдений час (для прискорення загальної роботи) та лічильник пакетів для кожного класу поведінки, він приймає рішення коли генерувати дані, що відповідають нормальній роботі або імітувати здійснення атаки. Після генерації пакета, він зберігається в тимчасовому масиві разом з позначкою, яка позначає клас для навчання. Після генерації усіх пакетів вони зберігаються в файли learning.csv та training.csv відповідно як набір даних для навчання та тренування.

Діаграма пакету для модуля моделювання зображена на рисунку 4.1.

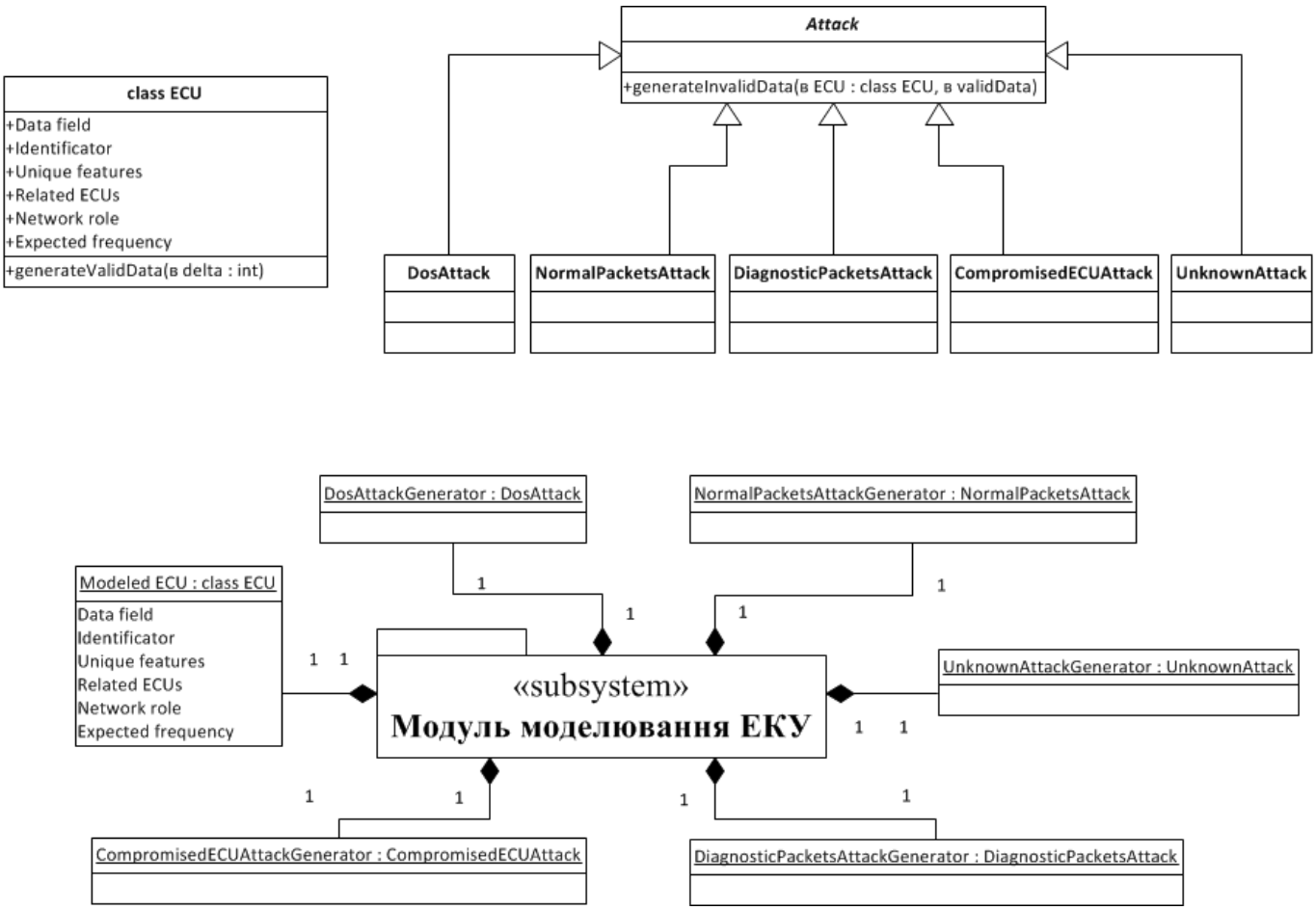

Рисунок 4.1 – Діаграма модуля моделювання

Система виявлення атак. Опис компонентів СВА надано в підрозділі 3.2. Архітектура компонентів СВА представлена на плакаті 4 додатку А. Далі наводиться короткий опис їх функціонального призначення в даній реалізації.

Детектор очікує на появу пакетів в віртуальній шині CAN. Ядро операційної системи Linux має у своєму складі драйвер з пакету SocketCAN [59]. Це дозволяє обмінюватися даними у форматі протоколу CAN за допомогою сокетів, що є де-факто стандартом для реалізації мережевих технологій для UNIX-подібних ОС.

Контекст мережі зберігає параметри кожної моделі ЕКУ з модуля моделювання та оновлює їх після генерації пакету нормальної поведінки.

Базою правил є нейронна мережа, а саме багатошаровий перцептрон. Він використовується у складі СВА виключно для класифікації вектора ознак, що формується після отримання пакета детектором. В даному випадку нейронна мережа

не тільки зберігає правила виявлення, але й додатково є детектором, що повинен виявити аномальну поведінку в мережі. БШП навчається після того як модуль моделювання створив дані. Після цього параметри БШП не змінюються під час роботи у складі системи виявлення атак.

Модуль прийняття рішень займається попереднім вилученням та збором даних для того, щоб сформувати вектор ознак для БШП. Він вилучає поле даних, ідентифікатор ЕКУ з пакета, отримує попередні значення параметрів ЕКУ, якому був надісланий пакет, обчислює різницю в часі між попередньою та поточною відправкою даних для ЕКУ-одержувача, запитує електричні характеристик ЕКУ-відправника і створює пакет того ж формату, що використовувався для навчання БШП

Система інформування в цій моделі виключно пише повідомлення в командний рядок у разі виявлення атак.

4.3 Порядок роботи програмного продукту

Розроблене програмне забезпечення створює дані для навчання, навчає БШП та перевіряє роботу СВА, що представляється наступним алгоритмом.

Крок 1. Ініціалізація об’єкта, що моделює ЕКУ, ініціалізація генераторів атак (об’єктів відповідних класів, що генерують дані для здійснення атаки).

Крок 2. Імітація роботи ЕКУ та здійснення атак, що здійснюється зверненням до моделі ЕКУ та генераторів атак для генерації відповідних даних. Кожна генерація відбувається з фіксованою або обчисленою частотою, що збільшує значення лічильника пройденого часу. Таким чином генерується 50000 пакетів для навчання та 10000 для тренування.

Крок 3. Взаємодія з БШП для його навчання та тренування. Результатом є вагові коефіцієнти зв’язків нейронів та кількість успішно виявлених класів поведінки.

Крок 4. Перевірка коректності роботи СВА з навченим БШП в якості детектора. Це можна здійснити двома способами. Використати дані згенеровані на кроці 2 починаючи з довільного пакету або згенерувати нові пакети використовуючи модуль моделювання ЕКУ. В цій роботі використовувався другий підхід.

Висновок до розділу 4

Даний розділ надає детальний опис вимог для розробки програмного продукту, перелік сторонніх бібліотек, що були використані для генерування пакетів протоколу CAN та навчання нейронної мережі. Розглянуті основні компоненти, їх складові частини та функціональне призначення. Наведено опис моделювання роботи ЕКУ та генерації даних для здійснення атак. Архітектура модуля моделювання представлена UML діаграмою.

Метою розробки програмного продукту було практичне використання запропонованих ознак для моделювання ЕКУ та виявлення атак за допомогою багатошарового перцептрону у складі системи виявлення атак.

ВИСНОВКИ

В рамках магістерської дисертації була розглянута поточна ситуація з інформаційною безпекою сучасних транспортних засобів. Було виявлено, що існуючі на ринку рішення надають широкі можливості для здійснення атаки зловмисником, це є результатом того, що існуючі рішення та їх архітектура проектувалися без врахування вимог інформаційної безпеки та того, що не існує загальних для індустрії стандартів таких, що відповідають сучасним вимогам та яких дотримуються усі виробники.

Огляд здійснення атак проти реальних автомобілів та окремих ЕКУ, аналіз їх результатів дозволив виявити два загальних типа атак. До першого типу належать атаки, які використовують дані для нормальної роботи ЕКУ, але з модифікованими значеннями та тоді, коли це необхідно зловмиснику, а не водію. Також було відзначено, що більшість дослідницьких робіт зосереджені на пошуку практичної можливості виконання неавторизованих дій, тоді як мало уваги привертається до систематизації та стандартизації отриманих результатів та заходів для підвищення рівня інформаційної безпеки.

Аналіз здійснення та наслідків атак був використаний для створення моделі загроз для автомобіля, де враховувалися 5 параметрів, що впливають на безпеку автомобіля, з оцінюванням проаналізованих атак для визначення рівня загроз, що вони представляють. Отримані оцінки загроз були використані для кількісної оцінки поверхні загроз для ЕКУ, що були об’єктом атак. Створені модель загроз та поверхні атак, їх оцінювання дали можливість визначити найсуворіші за наслідками атаки.

Аналіз атак також дав можливість визначити загальний алгоритм здійснення атак, що описує чисельні атаки на різні ЕКУ, визначити ознаки для створення математичної моделі ЕКУ, а саме параметри ЕКУ та його нормальну поведінку. Були створені чотири моделі з використанням отриманих ознак для моделювання принципово різних за роботою ЕКУ.

Були запропоновані архітектура багатошарового перцептрона та його параметрів для його використання в якості бази правил та детектора у складі системи виявлення атак. Отримана точність виявлення атак є задовільною.

Необхідно виділити наступні заходи для подальшого дослідження.

Відсутність наборів даних отриманих під час роботи автомобіля обмежує можливості для створення бази правил та профілю користувача. В даній роботі використовувалися штучні дані та закон зміни цих даних такі, що є лише наближенням до реальних даних ЕКУ під час роботи автомобіля.

Відсутність інформації про архітектури ЕКУ та їх зв’язки у відкритому доступі. Ця інформація здебільшого не поширюється виробниками, а те, що є містить недостатньо інформації. Компанії виробники досі намагаються не розкривати якомога більше даних про роботу автомобіля, що є додатковою мотивацією для хакерів для здійснення атак.

Результати виявлення класів поведінки з використанням БШП свідчать про необхідність створення додаткових класів поведінки, оскільки існуючі є занадто загальними, що негативно позначається на точності виявлення. Створення класифікації та ієрархії атак є відкритим питанням, що дозволить створити більш точні правила виявлення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Чеканін О.Ю., Жданова О.Г. Модель загроз для оцінки безпеки автомобіля // Матеріали науково-практичної конференції «Інформатика та обчислювальна техніка ІОТ-2018». – м. Київ.: НТУУ «КПІ ім. Ігоря Сікорського», 23-24 квітня 2018.

2. A. Saad and U. Weinmann, “Automotive software engineering and concepts,” in GI Jahrestagung, pp. 318–319, Frankfurt, Germany, September-October 2003.

3. E. Nickel, “IBM automotive software foundry,” in Press Conference on Computer Science in Automotive Industry, Frankfurt University, Frankfurt, Germany, September 2003.

4. Kaspersky, E.: Viruses coming aboard?, Viruslist.com – Режим доступу до ресурсу: http://www.viruslist.com/en/weblog?discuss=158190454&return=1.

5. [Електроний ресурс] Car-2-Car Communication Consortium (June 2008), http://www.car-2-car.org/

6. Hackers remotely kill a jeep on the highway—with me in it. – Режим доступу до ресурсу: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

7. Lang, A., Dittmann, J., Kiltz, S., Hoppe, T.: Future Perspectives: The Car and its IPAddress - A Potential Safety and Security Risk Assessment. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007. LNCS, vol. 4680. Springer, Heidelberg (2007).

8. Tobias Hoppe, Stefan Kiltz, and Jana Dittmann: Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures.

9. Guide to Intrusion Detection and Prevention Systems (IDPS) – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-94/final.

10. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security, Min-Joo Kang, Je-Won Kang.

11. Design and implementation of an intrusion detection system (IDS) for in-vehicle networks, Noräs salman, Marco bresch.

12. A Neural Network based system for Intrusion Detection and attack classification, Basant Subba , Santosh Biswas, Sushanta Karmakar

13. Neural Network based Intrusion Detection Systems, Sodiya A.S, Ojesanmi O.A, Akinola O.C, Aborisade O.

14. Neural Network Based Intrusion Detection System for Critical Infrastructures Ondrej Linda, Todd Vollmer, Milos Manic

15. Журнал Хакер 03 /194/ 2015, с.16-19.

16. Bus Systems – Режим доступу до ресурсу: https://automotive.softing.com/en/standards/bus-systems.html

17. Bosch CAN Specification version 2.0, Robert Bosch Gmbh, Postfach 50, D-7000 Stuttgart.

18. ISO 17987. Road vehicles - Local Interconnect Network (LIN) Part 1-7. ISO 17987:2016. Geneva, Switzerland: Internation Organization for Standardization, 2016.

19. ISO 17458. Road vehicles - FlexRay communications system Part 1-5. ISO 17458-5:2013. Geneva, Switzerland: Internation Organization for Standardization, 2013.

20. MOST Specification Rev 2.5 10/2006.

21. G Leen, D Heffernan, Expanding Automotive Electronic Systems, Computer, 3518893Jan. 2002 – Режим доступу до ресурсу: http://ltodi.est.ips.pt/malves/Gaveta/tme/can-automoveis.PDF

22. Technical Papers on the Development of Embedded Electronics, 6th Edition – Режим доступу до ресурсу: https://vector.com/portal/medien/cmc/marketing_items/ web/91102.pdf

23. ISO/IEC 7498-1. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994. Geneva, Switzerland: Internation Organization for Standardization, 1994.

24. Система виявлення атак – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IDS

25. Зоріна Т.І.

26. Системи виявлення і запобігання атак в комп’ютерних мережах / Т.І. Зоріна // Вісник Східноукраїнського національного університету імені Володимира

Даля. - 2013. - № 15(1). - С. 48-52. - Режим доступу: http://nbuv.gov.ua/UJRN/VSUNU_2013_15%281%29__9

27. Intrusion Detection Systems – Режим доступу до ресурсу: http://www.vce-download.net/study-guide/comptia-securityplus-2.4.1-intrusion-detection-systems.html

28. Сигнатура атаки – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.

29. Штучна нейронна мережа – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа.

30. Прогнозування за допомогою нейронних мереж – Режим доступу до ресурсу: wiki.tntu.edu.ua/Прогнозування_за_допомогою_нейронних_мереж.

31. Cannady, J. (1998) Artificial Neural Networks for Misuse Detection. National Information Systems Security Conference, 368-381.

32. Експертні системи – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Експертні_системи.

33. Wolf, M., Weimerskirch, A., Wollinger, T.: State of the Art: Embedding Security in Vehicles. EURASIP Journal on Embedded Systems 2007, 16 (2007); Article ID 74706, 16 pages, 2007. doi:10.1155/2007/74706

34. Ed Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Riskm 2015 – Режим доступу до ресурсу: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

35. K. Koscher et al., “Experimental security analysis of a modern automobile,” in Proceedings — IEEE Symposium on Security and Privacy, 2010, pp. 447–462

36. Циклічний надлишковий код – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Циклічний_надлишковий_код.

37. RFC2828. Shirey, R., "Internet Security Glossary", RFC 2828, DOI 10.17487/RFC2828, May 2000.

38. ISO/IEC, "Information technology - Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008.

39. Winsen, Stijn van, “Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles”, 2017 – Режим доступу до ресурсу: http://essay.utwente.nl/71792/.

40. Dr. Charlie Miller, Chris Valasek, “Adventures in Automotive Networks and Control Units” – Режим доступу до ресурсу: http://illmatics.com/car_hacking.pdf.

41. S. Checkoway et al., “Comprehensive experimental analyses of automotive attack surfaces”. In Proceedings of the 20th USENIX Conference on Security, SEC’11.

42. ISO 26262. Road vehicles – Functional safety. ISO 26262:2012. Geneva, Switzerland: Internation Organization for Standardization, 2012.

43. Draft NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

44. The STRIDE Threat Model – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

45. David Ward, Ireri Ibara, and Alastair Ruddle. “Threat Analysis and Risk Assessment in Automotive Cyber Security.” In: SAE International Journal of Passenger Cars-Electronic and Electrical Systems 6.2 (2013), pp. 507–513. ISSN: 1946-4622. DOI: doi:10.4271/2013-01-1415.

46. Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, 2015 – Режим доступу до ресурсу: https://www.govtrack.us/congress/bills/106/hr5164/text.

47. Defcon: Hacking Tire Pressure Monitors Remotely – Режим доступу до ресурсу: https://www.networkworld.com/article/2231495/cisco-subnet/defcon---hacking-tire-pressure-monitors-remotely.html.

48. Mauw, S., Oostdijk, M.: Foundations of Attack Trees. In Won, D., Kim, S., eds.: ICISC. Volume 3935 of LNCS., Springer (2005) 186–198.

49. Ishtiaq Roufa et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”. ISBN: 888-7-6666-5555-4.

50. Attack Surface Analysis Cheat Sheet – Режим доступу до ресурсу: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.

51. Pratyusa K. Manadhata, “An Attack Surface Metric”, November 2008.

52. AUTOSAR FO Release 1.3.0 Glossary – Режим доступу до ресурсу: https://www.autosar.org/fileadmin/user_upload/standards/foundation/1-3/AUTOSAR_TR_Glossary.pdf.

53. Real-Time Systems, Stefan M. Petters – Режим доступу до ресурсу: http://www.cse.unsw.edu.au/~cs9242/08/lectures/09-realtimex2.pdf

54. Ключевые рекомендации по глубокому обучению (Часть 2) – Режим доступу до ресурсу: http://datareview.info/article/eto-nuzhno-znat-klyuchevyie-rekomendatsii-po-glubokomu-obucheniyu-chast-2.

55. The Python Tutorial – Режим доступу до ресурсу: https://docs.python.org/3/tutorial/index.html

56. python-can – Режим доступу до ресурсу: https://python-can.readthedocs.io/en/stable/.

57. NumPy – Режим доступу до ресурсу: http://www.numpy.org/.

58. TensorFlow – Режим доступу до ресурсу: https://www.tensorflow.org/.

59. Keras: The Python Deep Learning library – Режим доступу до ресурсу: https://keras.io/.

60. SocketCAN – Режим доступу до ресурсу: https://www.kernel.org/doc/Documentation/networking/can.txt.